产品指南

VirusScan Enterprise

7.0 版



版权

© 2003 Networks Associates Technology, Inc. 保留所有权利。
未经 Networks Associates Technology, Inc. 或其供应商或子公司的书面许可，不得以任何形式或手段将本出版物的任何部分复制、传播、转录、存储在检索系统中或翻译成任何语言。要获得该许可，请写信给 Network Associates 法律部门，通信地址为：3965 Freedom Circle, Santa Clara, California 95054，或致电 +1-972-308-9960。

商标归属

Active Firewall、 Active Security、 Active Security （日语片假名）、 ActiveHelp、 ActiveShield、AntiVirus Anyware 及图案、 Bomb Shelter、 Certified Network Expert、 Clean-Up、 CleanUp Wizard、 CNX、 CNX Certification Certified Network Expert 及图案、 Design （N 风格）、 Disk Minder、Distributed Sniffer System、Distributed Sniffer System（日语片假名）、Dr Solomon's 标签、Enterprise SecureCast、Enterprise SecureCast（日语片假名）、Event Orchestrator、EZ SetUp、First Aid、ForceField、GMT、GroupShield、GroupShield（日语片假名）、Guard Dog、HelpDesk、HomeGuard、Hunter、LANGuru、LANGuru（日语片假名）、M 及图案、Magic Solutions、Magic Solutions （日语片假名）、 Magic University、 MagicSpy、 MagicTree、 McAfee、 McAfee （日语片假名）、 McAfee 及图案、 McAfee.com、 MultiMedia Cloaking、 Net Tools、 Net Tools（日语片假名） 、 NetCrypto、 NetScan、 NetShield、 NetStalker、 Network Associates、 NetXray、NotesGuard、 Nuts & Bolts、 Oil Change、 PC Medic、 PCNotary、 PrimeSupport、 Recoverkey、Recoverkey - International、 Registry Wizard、 ReportMagic、 Router PM、 Safe & Sound、SalesMagic、SecureCast、Service Level Manager、ServiceMagic、SmartDesk、Sniffer、Sniffer（朝鲜语）、Stalker、SupportMagic、TIS、TMEG、Total Network Security、Total Network Visibility、Total Network Visibility（日语片假名）、Total Service Desk、Total Virus Defense、Trusted Mail、UnInstaller、Virex、Virus Forum、ViruScan、VirusScan、WebScan、WebShield、WebShield（日语片假名）、WebSniffer、WebStalker、WebWall、Who's Watching Your Network、WinGauge、Your E-Business Defender、 ZAC 2000、 Zip Manager 是 Network Associates, Inc 和 / 或其子公司在美国和/或其他国家的注册商标。本文档中所有其他注册和未注册的商标均为其各自所有者专有。

本产品包括或可能包括由 OpenSSL Project 开发的，用于 OpenSSL Toolkit 的软件。
(http://www.openssl.org/)

本产品包括或可能包括由 Eric Young 编写的加密软件。(eay@cryptsoft.com)

许可协议

所有用户请注意：请仔细阅读与您所购买的许可权相关的适当的法律协议（下称“本协议”），本协议规定了使用被许可软件的一般条款和条件。如果您不知道您所购买的许可权是哪一类的，请参看您的软件包装盒随附的或您购买时另行得到的销售和其他有关的许可权授与或订购文件（作为书签、产品光盘上的文件或下载软件包的网站）。如果您不同意本协议规定的所有条款和条件，请勿安装软件。如果适用，您可以将产品退回 NETWORK ASSOCIATES 或原购买处以获得全额退款。

目录

前言

本产品指南为您介绍了 McAfee VirusScan® Enterprise 7.0 版，并提供了下列信息：

- 本版软件中所有新功能的说明。
- 所有产品功能的说明。
- 配置及部署本软件的详细说明。
- 执行各种任务的操作。
- 关于如何获取附加信息或帮助的说明。

读者

这些信息主要面向两种读者：

- 负责公司防病毒和安全程序的网络管理员。
- 负责更新工作站上病毒定义 (DAT) 文件或配置本软件检测选项的用户。

获取更多信息

安装指南

安装和启动本软件的系统要求和指导。

以产品光盘附带的印刷手册形式提供。另外，也可从产品光盘或 McAfee 下载站点获得 Adobe Acrobat .PDF 格式的文件。

帮助

帮助系统中的产品信息可以从应用程序中获得。

- 帮助系统可以提供高级且详细的信息。
- 上下文相关帮助（这是什么？）提供应用程序中选定内容的帮助。右键单击某个选项，按 [F1] 控制键，或将问号拖放到某个选项上。

版本指南

本版本产品的新增功能和修订功能的高级说明。

配置指南

与 ePolicy Orchestrator 配合使用。通过 ePolicy Orchestrator 管理软件来安装、配置、部署和管理 McAfee 产品的步骤。

从产品光盘或McAfee下载站点可以获得Adobe Acrobat .PDF 格式的文件。

发行说明

自述文件。产品信息、系统要求、已解决的问题、任何已知问题以及对该产品或其文档的最近增补或修订。

从产品光盘或 McAfee 下载站点可以获得 .TXT 格式的文件。

联系

Network Associates 驻美国及全球办事处的电话号码、街道地址、网址和传真号码列表。此外，还有服务部门与资源部门的联系信息，包括：

- 技术支持
- 客户服务
- 下载支持
- AVERT 防病毒紧急响应小组
- McAfee 测试站点
- 现场培训
- Network Associates 全球办事处

与 McAfee 和 Network Associates 联系

技术支持	http://knowledge.nai.com
McAfee 测试站点	www.mcafeeb2b.com/beta/
AVERT 防病毒紧急响应小组	www.mcafeeb2b.com/naicommon/avert/default.asp
下载站点	www.mcafeeb2b.com/naicommon/download/default.asp
DAT 文件更新	www.mcafeeb2b.com/naicommon/download/dats/find.asp
	ftp://ftp.nai.com/pub/antivirus/datfiles/4.x
产品升级	www.mcafeeb2b.com/naicommon/download/upgrade/login.asp

需要有效的授权号。
与 Network Associates 客户服务部门联系。

现场培训	www.mcafeeb2b.com/services/mcafee-training/default.asp

Network Associates 客户服务部门：

电子邮件	services_corporate_division@nai.com
Web	www.nai.com
	www.mcafeeb2b.com

美国、加拿大和拉丁美洲免费电话：

电话	+1-888-VIRUS NO　或　+1-888-847-8766
	星期一到星期五，中部时间上午 8:00 - 下午 8:00

McAfee 非常重视客户的反馈意见，并愿意根据客户的反馈信息改进我们的解决方案。如果您对 McAfee 产品中的语言问题存在任何意见或建议，请给我们发送电子邮件，地址如下：

B2BLoc_ZH-CN@nai.com

有关与 Network Associates 和 McAfee 联系的更多信息 （包括其他地区的免费电话号码），请参阅本产品附带的 Contact 文件。

关于 VirusScan Enterprise 1

VirusScan Enterprise 7.0 软件能够帮助您轻松控制扫描操作。您可以将本地和网络驱动器以及电子邮件和附件指定为扫描目标，通知该应用程序如何响应发现的所有病毒，还可以生成应用程序操作报告。

VirusScan Enterprise 软件既支持服务器也支持工作站，以及众多的第三方应用程序。它是如下软件的替代品：

- VirusScan 4.5.1 工作站版本。
- NetShield NT 4.5 服务器版本。
- 适用于 Celerra™ 文件服务器的 NetShield for Celerra™ 4.5 版本。

本产品指南为您提供了配置和使用 VirusScan Enterprise 软件的相关信息。有关系统要求和安装说明，请参阅 《VirusScan Enterprise 安装指南》。

这部分包含下列主题：

- 本版本的新功能
- 产品功能

本版本的新功能

本版本的 VirusScan Enterprise 产品引入了下列新功能：

- 集文件服务器和桌面机配置功能于一身。
- 本产品的英语版本可运行在本地化后的操作系统中。
- 全面支持 Microsoft Windows 2000 和 Windows .NET 高级功能：
  - Active Directory。
  - 集群服务 - 主动 / 主动与主动 / 被动。
  - 终端服务。
- 支持 Microsoft .NET Server 操作系统。
- 与第三方产品兼容。本 VirusScan Enterprise 软件兼容许多第三方应用程序，这意味着：
  - 即便存在其他应用程序，VirusScan Enterprise 的安装也丝毫不受影响。
  - 它仍然能够正常执行扫描、更新、报告和报警，性能不会下降。
  - 在正常使用的情况下，也不会对其他应用程序的效用造成不良影响。
- 强化的更新功能：
  - 可自动更新完整病毒定义 (DAT) 文件、增量 DAT、EXTRA.DAT、引擎以及 HotFix 等文件。
  - 可同时对桌面机和服务器进行镜像更新。
  - 通过 HTTP、FTP（被动或主动）、UNC 共享、本地驱动器或映射驱动器进行更新。
  - 配置延迟更新的能力。
  - 能够在传输中断后恢复更新。
  - 单击 “**立即更新**” 即可开始更新。
- 强化的扫描功能：
  - 更快速的扫描性能。
  - 改进的检测文件是否已扫描过的功能。
  - 可恢复的按需扫描。
  - 用于低风险和高风险应用程序的扫描选项。
- 改进的安全性，可限制最终用户访问界面。

产品功能

本 VirusScan Enterprise 软件包含多种功能。所有功能共同构成了计算机防御病毒和其他恶意软件攻击的屏障。这些功能包括：

- **VirusScan 控制台**。控制台是一个控制点，允许您创建、配置和运行 VirusScan Enterprise 任务。任务可包含任何操作，例如从按照指定时间或时间间隔在一组驱动器上运行扫描操作，或者运行更新操作。还可从控制台启用或禁用 VShield 扫描程序。请参阅第 18 页的 “VirusScan 控制台”。

- **按访问扫描程序**。该功能可为您提供连续的防病毒保护，以防范来自软盘、网络或 Internet 上各种病毒来源中的病毒。它在计算机启动时启动，并驻留在内存中，直到系统关闭。您可以使用一组灵活的属性页来通知扫描程序要检查系统的哪些部分、查找哪些内容、忽略哪些部分以及如何处理发现的感染病毒文件。此外，这种扫描程序可在发现病毒时向您发出警报，并为每个操作生成摘要报告。

  该功能在安装本软件时已完全配置，但您仍可以根据安全需要重新配置它。请参阅第 33 页的 “按访问扫描”。

- **按需扫描程序**。使用该功能，您可以随时开始扫描、指定扫描和不扫描的目标、确定扫描程序在检测到病毒时的响应方式以及查看病毒事件报告和警报。此外，也可以创建在特定时间或特殊时间间隔内进行的扫描任务。还可以定义所需的各种按需扫描任务，然后保存配置好的任务，以便重新使用。请参阅第 63 页的 “按需扫描”。

- **电子邮件扫描程序**。该功能允许扫描 Microsoft Outlook 邮件、附件或者可以在计算机中直接访问的公共文件夹。如果正在运行 Outlook，则将按发送扫描电子邮件。您也可以随时执行按需电子邮件扫描。这一功能使您能够在病毒进入您的电脑之前就发现潜在的病毒。请参阅第 89 页的 “电子邮件扫描”。

- **自动更新**。该功能允许您自动更新病毒定义 (DAT) 文件和扫描引擎，然后将这些更新分发给网络中的计算机。您也可以借助该功能下载Hotfix和产品升级。根据网络的规模，您可以指定一台或多台信任的计算机（包括贵公司内部的 HTTP 站点主机）自动从 Network Associates HTTP 站点下载新文件。请参阅第 153 页的 “更新”。

- **警报管理器**。警报管理器与 VirusScan Enterprise 产品分开安装。安装后，通过配置该功能，就可以在扫描程序检测到计算机病毒时获得通知。您可以选择由警报管理器实用程序通过电子邮件、打印机、 SNMP 陷阱或其他方式通知您。默认情况下，警报管理器未经预先配置，所以必须首先配置警报管理器，才能接收或发送病毒警报消息。详细说明，请参阅第 117 页的 “病毒警报”。

- **命令行扫描程序**。您可以使用本功能，从 “**命令提示**” 对话框初始化目标扫描操作。SCAN.EXE 是一个只用于 Windows NT 环境的扫描程序，也是主要的命令行界面。

  通常情况下，您会使用 VirusScan Enterprise 用户界面执行大部分扫描操作，但如果在启动 Windows 时遇到问题，或 VirusScan Enterprise 功能无法在您的环境中运行时，可以将命令行扫描程序作为备用方法使用。请参阅第 191 页的 “命令行扫描程序”。

入门 2

安装 VirusScan Enterprise 软件后，您可以配置它的组件。

这部分包含下列主题：

- 面向用户的界面
- 设置用户界面选项
- 设置扫描操作
- 病毒信息库
- 提交病毒样本
- 设置远程管理

面向用户的界面

VirusScan Enterprise 软件为您提供了运用多种不同方法执行操作的灵活性。尽管具体细节有所不同，但很多操作都可以从控制台、工具栏、菜单或桌面进行。以下章节为您详细介绍每种方法

这部分包括以下界面：

- 开始菜单
- VirusScan 控制台
- 右键单击菜单
- 系统任务栏
- 命令行

开始菜单

使用 “**开始**” 菜单：

- 如果安装了警报管理器，可以从这里访问警报管理器配置。
- 访问 “**VirusScan 控制台**”。
- 打开按访问扫描属性页。
- 打开按需扫描属性页。这是一种不保存的一次性按需扫描。

单击“**开始**”按钮，选择“**程序**”|“**Network Associates**”，然后选择所需的组件。

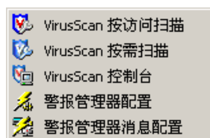


图 2-1. VirusScan - 开始菜单

VirusScan 控制台

“**VirusScan 控制台**”是所有程序活动的控制点。

使用以下方法之一打开 “**VirusScan 控制台**”：

- 单击“**开始**”按钮，选择“**程序**”|“**Network Associates**”|“**VirusScan 控制台**”。
- 右键单击系统任务栏中的 ，然后选择 “**VirusScan 控制台**”。

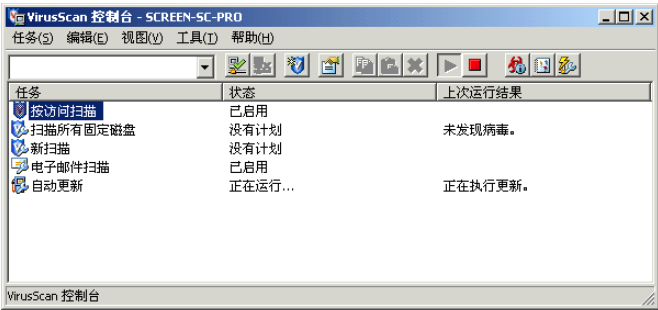


图 **2-2. VirusScan** 控制台

这部分包含下列主题：

- 菜单栏
- 工具栏
- 任务列表
- 状态栏

菜单栏

“**VirusScan 控制台**”所包含的命令允许您远程连接 VirusScan Enterprise 计算机或断开与它的连接，创建、删除、配置、运行、停止和复制扫描任务，以满足极为严格的安全需求。所有这些命令都可从菜单中找到。此外，右键单击“**VirusScan 控制台**”中的任务，也可以找到某些命令。菜单概述如下。

这部分包含下列菜单：

- 任务菜单
- 编辑菜单
- 视图菜单
- 工具菜单
- 帮助菜单

任务菜单

使用“**任务**”菜单，可以创建和配置任务、查看统计信息、活动日志以及任务属性。



图 **2-3.** 任务菜单

注释

本菜单中的 “**禁用**”、“**删除**”、“**重命名**”、“**统计信息**”、“**活动日志**” 和 “**属性**” 可应用于所选的任务。

编辑菜单

使用 “**编辑**” 菜单，可以复制和粘贴任务。

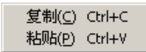


图 **2-4.** 编辑菜单

视图菜单

您可以从 “**视图**” 菜单中指定是否显示工具栏和状态栏，或者刷新控制台。

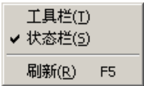


图 **2-5.** 视图菜单

工具菜单

您可以在 “**工具**” 菜单中配置警报、启动事件查看器、指定用户界面选项、锁定或解锁用户界面安全性、在配置远程控制台时连接或断开计算机连接、导出或编辑站点列表以及将 DAT 文件恢复为前一个版本。



图 **2-6.** 工具菜单

帮助菜单

使用 “**帮助**”菜单，可以访问联机帮助主题、病毒信息库或技术支持网站。还可以向防病毒紧急响应小组 (AVERT) 提交病毒样本。“**关于**”对话框则提供了产品、DAT 文件版本和扫描引擎的相关信息。

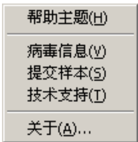


图 **2-7.** 帮助菜单

工具栏

您只需单击工具栏图标，就可以快速使用很多命令。这些图标包括：

- 连接到计算机。
- 断开与计算机的连接。
- 创建新任务。
- 显示所选项的属性。
- 复制所选项。
- 粘贴所选项。
- 删除所选项。
- 启动所选项。
- 停止所选项。
- 访问病毒信息库。
- 打开事件查看器。

配置警报选项。

任务列表

控制台包括 VirusScan Enterprise 可以执行的任务列表。任务是一组命令，用来按照特定的配置、在特定时间运行特殊的程序或扫描操作。

要配置某个任务，请选择该任务并单击 ，或者双击该任务以打开它的属性页。VirusScan Enterprise 软件附带以下默认任务：

- **按访问扫描**。这是一种自动按访问扫描任务。该任务是唯一的，不能被复制。要了解如何配置按访问扫描，请参阅第 33 页的 “按访问扫描”。
- **电子邮件扫描**。这是一种按发送电子邮件扫描任务。该任务是唯一的，不能被复制。要了解如何配置按发送或按需电子邮件任务，请参阅第 89 页的 “电子邮件扫描”。
- **自动更新**。这是一种按需更新任务。为满足需求，您可以在使用这一默认更新任务之外，创建其他按需更新任务。要了解如何创建和计划更新任务，请参阅第 153 页的 “更新”。
- **扫描所有固定磁盘**。这是一种按需扫描任务。为满足需求，您可以在使用这一默认按需扫描任务之外，创建其他扫描任务。要了解如何创建、配置和计划按需任务，请参阅第 63 页的 “按需扫描”。

状态栏

状态栏显示当前活动的状态。

右键单击菜单

通过右键单击菜单，可以快速使用常用的操作，例如创建新任务、查看任务统计信息和日志、打开任务属性页或者扫描特定的文件或文件夹。

- **右键单击控制台菜单**。“**VirusScan 控制台**”提供的右键单击菜单不尽相同，这主要取决于是否选择了任务列表中的任务以及选择了哪些任务。详细信息，请参阅第 22 页的 “右键单击控制台菜单”。
- **右键单击扫描**。右键单击扫描功能允许您选择特定的文件或文件夹并立即开始扫描病毒。详细信息，请参阅第 23 页的 “右键单击扫描”。
- **从系统任务栏右键单击扫描**。详细信息，请参阅第 23 页的 “从系统任务栏右键单击扫描”。

右键单击控制台菜单

右键单击任务列表中的项目，可获得如下选项：

- **按访问扫描**。如果右键单击任务列表中的按访问扫描任务，可以禁用此任务、查看任务统计信息、查看活动日志以及打开属性页。

- **更新**。通过右键单击任务列表中的更新任务，您可以启动、删除和重命名这个任务、查看任务日志以及打开属性页。
- **电子邮件扫描**。右键单击任务列表中的电子邮件扫描任务，您可以禁用此任务、查看任务统计信息、查看活动日志以及打开属性页。
- **按需扫描**。通过右键单击任务列表中的按需扫描，您可以启动、复制或粘贴、删除、重命名这个任务、查看任务统计信息、活动日志以及打开属性页。

无需选择任务列表中的项目，只要右键单击控制台中的空白区域即可执行下列操作：

- **新建扫描任务**。创建新的按需扫描任务。
- **新建更新任务**。创建新的更新任务。
- **新建镜像任务**。创建新的镜像任务。
- **粘贴**。把复制的任务粘贴到任务列表中。
- **用户界面选项**。访问 “**用户界面选项**” 属性页。有关设置用户界面选项的信息，请参阅第 24 页的 “设置用户界面选项”。

右键单击扫描

简单地在 Windows 资源管理器中右键单击文件或文件夹，然后选择 “**扫描病毒**”，就可以对其执行立即扫描。这也被称作 shell 扩展扫描。按需扫描程序可以直接调用，它将启用所有扫描设置，如存档扫描、启发式扫描等。

如果找到染毒的文件或文件夹，会以列表形式列出，并在扫描对话框底部显示染毒项目的详细说明。通过右键单击列表中的染毒项目，可以选择清除、删除或移动，对其采取措施。

执行右键单击扫描时，不能自定义扫描选项。若要自定义扫描选项，可以创建新的按需扫描任务。更多信息，请参阅第 64 页的 “创建按需扫描任务”。

系统任务栏

默认情况下，典型安装将安装按访问扫描程序，且该程序会自动激活。一旦激活，该扫描程序会在 Windows 系统任务栏中显示盾牌图标 。

双击系统任务栏中的 可查看 “**按访问扫描统计信息**”。

从系统任务栏右键单击扫描

右键单击系统任务栏中的 ，以显示菜单。



图 **2-8.** 系统任务栏菜单

系统任务栏菜单包括如下选项：

- **VirusScan 控制台**。显示 “**VirusScan 控制台**”。
- **禁用按访问扫描**。停止按访问扫描程序。这项功能可根据所选的操作切换。选择菜单中的 “**禁用按访问扫描**”之后，这一项的状态将变为 “**启用**” 。要重新激活扫描程序，请选择菜单中的 “**启用**”。
- **按访问扫描属性**。打开按访问扫描属性页，以从中配置按访问扫描程序。
- **按访问扫描统计信息**。查看按访问扫描程序消息。可以启用或禁用按访问扫描程序或打开按访问扫描程序属性页。
- **按访问扫描消息**。查看按访问扫描程序消息。您可以删除消息、清除文件、删除文件或移动文件。
- **按需扫描**。打开按需扫描程序属性页，从中可以执行不保存的一次性按需扫描。
- **立即更新**。立即更新默认的更新任务。

  注释
  “**立即更新**”仅对在安装本产品时创建的默认更新任务有效。您可以重命名和重新配置默认的更新任务，但如果删除了该默认任务，“**立即更新**”将随即被禁用。

- **关于 VirusScan Enterprise**。查看病毒定义文件、扫描引擎版本号以及产品许可信息。

命令行

您可以使用命令行组件从命令提示符执行操作。更多信息，请参阅第 191 页的 “命令行扫描程序”。

设置用户界面选项

在安装该程序时，您可以使用 McAfee Installation Designer 指定显示和密码选项，或者在安装后从 “**VirusScan 控制台**”的 “**工具**”菜单指定这些选项。

这部分描述了如何从控制台设置显示选项和密码选项。这部分包含下列主题：

- 显示选项
- 密码选项
- 解锁与锁定用户界面

显示选项

“**显示选项**”对话框允许您决定用户可访问哪些系统任务栏选项并设置本地控制台的刷新时间。

从控制台设置显示选项：

1 打开“**VirusScan 控制台**”。有关说明，请参阅第 18 页的“VirusScan 控制台”。

2 选择“**工具**”|“**用户界面选项**”|“**显示选项**”。

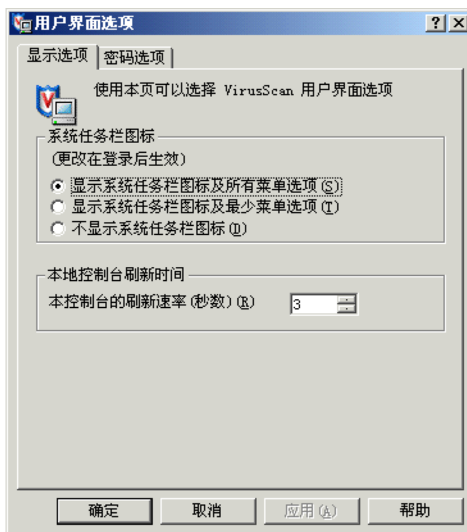


图 **2-9.** 显示选项

3 决定用户可见的系统任务栏选项。在“**系统任务栏图标**”下，选择一个选项：

- **显示系统任务栏图标及所有菜单选项**。该选项为默认选项。允许用户看到系统任务栏的所有菜单选项。

- **显示系统任务栏图标及最少菜单选项**。将右键单击菜单项的结果限制为只出现“**关于**”和“**按访问扫描统计信息**”项。所有其他右键单击菜单项都将隐藏。
- **不显示系统任务栏图标**。不允许用户访问系统任务栏图标。

4 在“**本地控制台刷新时间**”区域中，选择以秒为单位的控制台屏幕刷新频率。

5 单击“**应用**”，然后单击“**确定**”保存所做的更改并关闭该对话框。

密码选项

“**密码选项**”对话框允许您设置整个系统的安全密码，或者只为所选选项卡和控件设置安全密码。同一密码应用于所有选定的选项卡和控件。

设置密码将对用户产生以下影响：

非管理员 - 不具有 Windows NT 管理权限的用户。非管理员总是以只读模式运行所有 **VirusScan Enterprise** 应用程序。他们可以查看某些配置参数、运行以前保存的扫描任务以及运行立即扫描与更新，但不能更改任何配置参数或者创建、删除或修改以前保存的扫描与更新任务。

管理员 - 具有 Windows NT 管理权限的用户。如果尚未设置密码，管理员可以以读 / 写模式运行所有 VirusScan Enterprise 应用程序。他们可以查看和修改所有配置参数、运行任务、创建、删除和修改以前保存的扫描与更新任务。如果已经设置了密码，那么如果没有输入安全密码，管理员将只能以只读模式查看受保护的选项卡和控件。管理员还可以通过控制台锁定或解锁用户界面。更多信息，请参阅第 28 页的 “解锁与锁定用户界面”。

注释
一个锁住的红色挂锁表示这一项需要输入密码才能使用。开启的绿色挂锁表示这一项处于可以读 / 写的状态。

从控制台设置密码选项：

1 打开 “**VirusScan 控制台**”。有关说明，请参阅第 18 页的 “VirusScan 控制台”。

2 选择 “**工具**” | “**用户界面选项**” | “**密码选项**”。

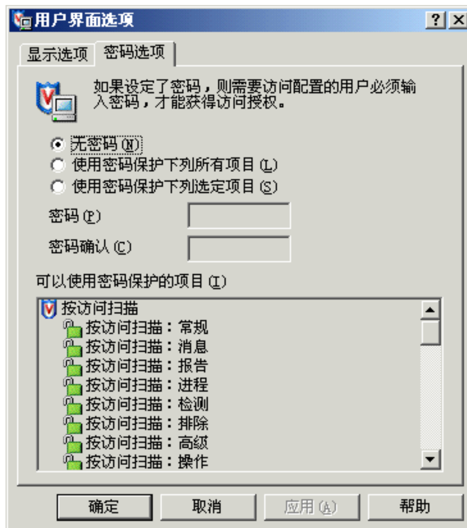


图 **2-10.** 密码选项

3. 选择以下选项之一：

   - **无密码**。该选项为默认选项。
   - **使用密码保护下列所有项目**。用户必须输入指定的密码，才能使用本软件中锁定的任何选项卡或控件。
     - 选择 “**使用密码保护下列所有项目**”。
     - 输入并确认密码。
   - **使用密码保护下列选定项目**。用户必须输入指定的密码，才能使用此处锁定的项目。未锁定的项目则不要求密码。
     - 选择 “**使用密码保护下列选定项目**”。
     - 输入并确认密码。
     - 选择受此密码保护的所有项目。

4. 单击 “**应用**” 保存更改。
5. 单击 “**确定**”。

解锁与锁定用户界面

管理员可以从控制台解锁和锁定密码保护的选项卡和控制。

> **注释**
> 如果为所有项目都选择了密码保护，则 “**用户界面选项**” 对话框也会自动受到保护。如果为所有项目都设置了密码保护且用户退出了系统，则用户界面会再次自动锁定。

解锁用户界面：

1. 打开 “**VirusScan 控制台**”。有关说明，请参阅第 18 页的 “VirusScan 控制台”。
2. 选择 “**工具**”。
3. 选择 “**解锁用户界面**”。

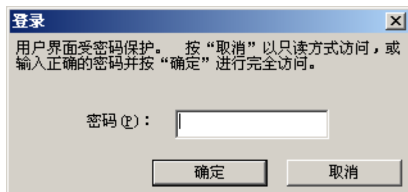


图 **2-11.** 安全密码

4. 输入密码。
5. 单击 “**确定**”。

锁定用户界面：

1. 打开 “**VirusScan 控制台**”。有关说明，请参阅第 18 页的 “VirusScan 控制台”。
2. 选择 “**工具**”。
3. 选择 “**锁定用户界面**”。

设置扫描操作

本 VirusScan Enterprise 软件提供可满足不同需要的不同扫描类型。

这部分包含下列主题：

- 按访问扫描与按需扫描的比较
- 自动扫描

- 定期、选择性或按计划扫描

按访问扫描与按需扫描的比较

VirusScan Enterprise 软件可执行两种类型的扫描活动。这两种扫描活动分别是：

- 自动扫描
- 定期、选择性或按计划扫描

按访问扫描。自动扫描病毒被称作按访问扫描。您必须具有管理权限才能配置这种扫描。更多信息，请参阅第 29 页的 "自动扫描"。

按需扫描。定期、选择性或事先计划的扫描称作按需扫描。您必须具有管理权限才能计划按需扫描任务，但是所有用户都能够运行这种任务。更多信息，请参阅第 30 页的 "定期、选择性或按计划扫描"。

按访问扫描程序能够以后台扫描方式持续地保护计算机，因此看起来运行按需扫描任务似乎是多余的。但是，良好的防病毒安全措施应同时包括彻底、定期的系统扫描，这是因为：

- **按访问扫描操作在访问或使用文件时检查文件**。按访问扫描程序只查找使用中的文件的病毒。如果有的文件很少使用但已经感染病毒，按访问扫描程序也只在文件使用时才会对其进行检测。但是，按需扫描操作可以检查硬盘上文件中的病毒，即使您未使用它们也是如此。因此，按需扫描操作可以在您使用文件之前检查它们的病毒。

- **意外的病毒**。如果在启动计算机时软盘还意外地留在驱动器中，就可能在按访问扫描程序检测之前将病毒加载到内存中，特别是如果未将扫描程序配置为扫描软盘时。一旦进入内存，恶性病毒就几乎可以感染所有程序。

- **按访问扫描占用时间和资源**。在运行、复制或保存文件时扫描病毒，会延迟软件启动时间和其他任务。根据具体情况，对于重要工作，耽搁这点时间可能是值得的。虽然影响非常小，但如果需要将全部可用的资源用于某些紧迫的任务，则可以禁用按访问扫描。在这种情况下，应在空闲期间执行定期扫描操作，这样既能够防止系统感染病毒，又不会影响工作效率。

- **安全措施越多越好**。如今，大多数计算机用户所在的环境都以连网的网络为中心，从某个来源下载病毒只需片刻时间，您甚至都意识不到自己访问过该来源。此时，如果由于软件冲突而暂时禁用了后台扫描，或尚未配置后台扫描来监视易受攻击的进入点，就可能染上病毒。定期扫描操作通常可在病毒传播或造成损害之前将其捕获。

自动扫描

根据用户的活动，按访问扫描可以提供连续实时的病毒检测和响应。 VirusScan Enterprise 防病毒软件程序提供单个按访问扫描任务，即在网络用户每次向计算机写文件或从计算机读取文件时检查病毒。它将尝试清除找到的所有病毒，并在日志文件中记录它的活动。更改它的设置可以确定：

- 要扫描的文件和文件类型。

- 执行扫描的突发条件。
- 扫描程序在检测到病毒后采取的操作。
- 扫描程序活动报告的内容 （如果有）。
- 排除在按访问扫描范围以外的文件。

有关按访问扫描的详细说明，请参阅第 33 页的 “按访问扫描”。

定期、选择性或按计划扫描

按需扫描任务共有两种类型：

- 不保存的一次性按需扫描任务。
- 可保存的按需扫描任务。

用户可以配置和预先计划不保存的一次性按需扫描任务，但它不能保存下来供日后使用，除非您选择保存它。

您可以预先计划可保存的按需扫描任务，并在认为必要时或按计划定期运行。您可以针对网络中的特殊位置创建任意多个扫描任务。这个特殊位置可以小范围地定义为特定的驱动器、文件夹或文件，也可以泛泛地定义为多个驱动器、文件夹或文件。一旦创建了可保存的扫描任务，则只能从 “**VirusScan 控制台**”中将它们删除，否则就一直可用。也可以根据需要编辑它们。

有关设置按需扫描活动的完整论述，请参阅第 63 页的 “按需扫描”。

病毒信息库

McAfee 防病毒紧急响应小组 (AVERT) 的病毒信息库包含关于病毒来源、系统如何感染以及如何删除的详细信息。

除真正的病毒外，病毒信息库还包含关于欺骗性病毒的有用信息以及关于能够摧毁硬盘的电子邮件附件的危险电子邮件警告。 Virtual Card For You 和 SULFNBK 是众多欺骗性病毒中最臭名昭著的两个。下次收到善意的病毒警告时，请在将邮件发给朋友之前先查看我们的欺骗性病毒网页。

访问病毒信息库：

1. 打开 “**VirusScan 控制台**”。有关说明，请参阅第 18 页的 “VirusScan 控制台”。

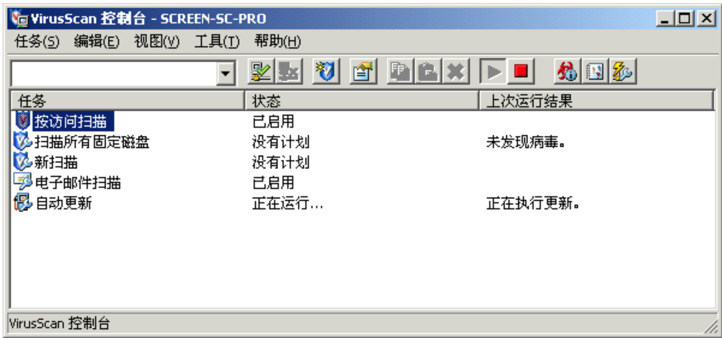


图 2-12. VirusScan 控制台

2 选择 “**帮助**” 菜单中的 “**病毒信息**”。

提交病毒样本

如果怀疑某个文件含有病毒，或遇到可能由病毒感染造成的系统问题， McAfee 建议您向 McAfee 的防病毒研究小组发送一个样本以进行分析。提交之后，不但会开始分析，而且如有担保，还将对文件进行实时修复。

向 AVERT 提交病毒样本：

1 打开 “**VirusScan 控制台**”。有关说明，请参阅第 18 页的 “VirusScan 控制台”。

2 选择 “**帮助**” 菜单中的 “**提交样本**”。

3 按照网站上的指导进行操作。

设置远程管理

您可以执行的操作包括在远程计算机上修改或计划扫描或更新任务，启用或禁用按访问扫描程序。要这样做，您必须具有管理员权限并且运行远程注册服务。

注释
如果您不具有连接至远程计算机的管理员权限，您会收到错误消息 “用户权限不足，拒绝访问”。

启动 “**VirusScan 控制台**” 后，与您连接的计算机的名称将出现在 “**控制台**” 标题栏和 “**控制台**” 工具栏左侧的菜单中。如果与本地计算机连接，则该菜单最初为空。如果没有连接到网络中的任何计算机，标题栏将显示本地计算机的名称。

要管理安装有 VirusScan Enterprise 程序的远程计算机，请按照以下步骤进行：

1 从 “**工具**”菜单中，选择 “**远程连接**”，或者单击工具栏中的 。

屏幕上将显示 “**连接到远程计算机**”对话框。

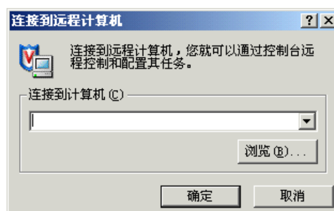


图 2-13. 连接到远程计算机

2 单击 并选择 “**连接到计算机**”列表中的计算机，或者在文本框中输入要管理的计算机名称。也可以单击 “**浏览**”查找网络中的计算机。

注释
如果配置用于远程任务的文件或文件夹路径名时使用了环境变量，请确保远程计算机上存在该环境变量。“**控制台**”无法验证远程计算机上的环境变量。

3 单击 “**确定**”尝试连接目标计算机。

注释
当与远程计算机连接后，标题栏会变化以反应出该计算机的名称，同时任务列表中的任务将变为供远程计算机使用的那些任务。用户可以为远程计算机添加、删除或重新配置任务。

“**控制台**”读取远程计算机的注册表，并显示远程计算机的任务。一旦任务出现在 “**控制台**”中，就可以在本地计算机上运行。

要断开与计算机的连接，请单击控制台任务栏中的 ，或者选择 “**工具**”菜单中的 “**断开计算机**”。断开与远程计算机的连接后，控制台会刷新以显示本地计算机的任务。

按访问扫描 3

VirusScan Enterprise 防病毒程序使用它的按访问扫描程序来根据您配置的设置持续、实时地检测和响应计算机上出现的病毒。该扫描程序在计算机启动时启动并持续进行扫描，直到系统关闭为止。

如果检测到病毒，按访问扫描程序将详细记录感染病毒文件的信息，并允许您快速访问该信息，然后立即对感染病毒的文件采取措施。

这部分包含下列主题：

- 配置按访问扫描程序
- 按访问扫描属性
- 常规设置
- 默认、低风险和高风险进程
- 查看扫描结果
- 响应病毒检测

配置按访问扫描程序

要确保该程序在您的计算机或网络环境中性能最佳，您需要通知该程序扫描什么、忽略什么、在发现病毒后如何处理，以及处理完毕后如何通知您。

按访问扫描程序的自带配置已启用了大多数响应属性。默认情况下，扫描程序被设置为发现病毒时予以清除。如果病毒无法清除，默认的辅助操作是隔离病毒。该程序还会把每个事件记录到日志文件中。

这部分包含下列主题：

- 按访问扫描属性
- 常规设置
- 默认、低风险和高风险进程
- 添加文件类型扩展名
- 添加用户指定的文件类型扩展名
- 排除文件、文件夹和驱动器

按访问扫描属性

要配置按访问扫描程序，请按以下步骤操作：

1 打开 "**VirusScan 控制台**"。有关说明，请参阅第 18 页的 "VirusScan 控制台"。

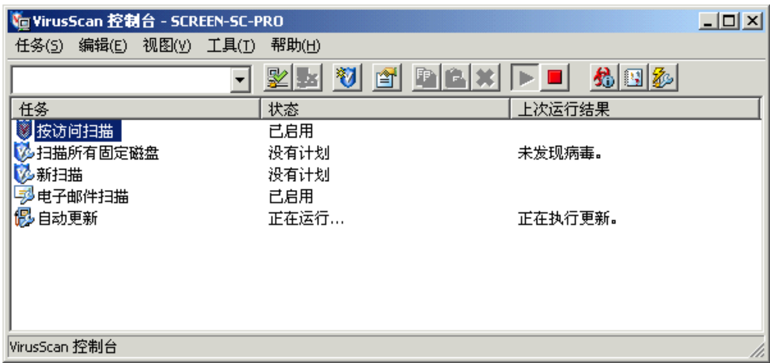


图 3-1. VirusScan 控制台

2 使用以下方法之一，打开 "**按访问扫描属性**"：

- 选择控制台 "**任务**" 菜单中的 "**按访问扫描属性**"。
- 右键单击控制台中的 "**按访问扫描**"，然后选择 "**属性**"。

- 双击控制台中的 “**按访问扫描**”。
- 突出显示控制台中的“**按访问扫描**”，然后单击控制台工具栏中的 。
- 右键单击系统任务栏中的 ，并选择 “**按访问扫描属性**”。
- 单击 “**开始**”按钮，然后选择 “**程序**” | “**Network Associates**” | “**VirusScan 按访问扫描**”。

屏幕上出现 “**按访问扫描属性**”页。



图 3-2. 按访问扫描属性 - 默认视图

初次打开 “**按访问属性**”页时，可以从默认视图访问 “**常规设置**”和 “**所有进程**”。

3 要设置“**低风险进程**”和“**高风险进程**”，请选择左侧窗格中的“**所有进程**”图标。“**常规**”、“**消息**”、和“**报告**”选项卡隐藏，屏幕上会出现“**进程**”、“**检测**”、“**高级**”和“**操作**”选项卡。

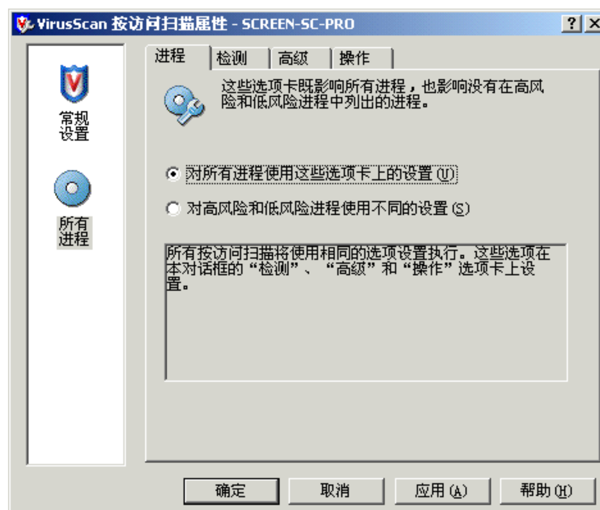


图 **3-3.** 按访问扫描属性 **-** 所有进程

4 选择“**进程**”选项卡中的“**对高风险和低风险进程使用不同的设置**”。

“**所有进程**”图标将变为“**默认进程**”，而且左侧窗格中的“**低风险进程**”和“**高风险进程**”图标均变为可用。



图 3-4. 按访问扫描属性

“**按访问扫描属性**”对话框允许您配置常规设置和三种类型的进程。可以使用该对话框左侧窗格中的图标访问以下各项的可配置选项：

- **常规设置**。关于所有进程的常规检测、消息和报告属性。在这里可以指定的属性不同于您为默认进程、低风险和高风险进程指定的属性。
- **默认进程**。默认情况下，该列表为空。所有未定义为低风险或高风险的进程都是默认进程。可以为默认进程指定的属性与可以为低风险和高风险进程指定的属性相同。
- **低风险进程**。引入或传播病毒的风险比较低的进程为低风险进程。可以为低风险进程指定的属性与可以为默认进程和高风险进程指定的属性相同。
- **高风险进程**。引入或传播病毒的风险比较高的进程为高风险进程。可以为高风险进程指定的属性与可以为默认进程和低风险进程指定的属性相同。

从该对话框左侧窗格中选择一个图标，然后依次单击每个选项卡指定扫描程序执行操作的方式。下一部分将介绍按访问扫描的可用属性。

常规设置

您指定的 “**常规设置**”属性将影响所有进程。

这部分包含下列主题：

- 常规属性
- 消息属性

- 报告属性

常规属性

使用 “**常规**”选项卡上的选项可以配置按访问扫描的常规属性。

1. 打开“**按访问扫描属性**”对话框，然后选择左侧窗格中的“**常规设置**”图标。
2. 选择 “**常规**”选项卡。



图 3-5. 常规设置 - 常规选项卡

3. 在 “**扫描**”区域中，选择扫描程序要检查计算机的哪些部分。从以下选项中进行选择：

   - **引导区**。该选项为默认选项。将磁盘引导扇区包括在扫描活动范围内。如果有磁盘，扫描程序会扫描磁盘引导扇区。在某些情况中，如果磁盘包含无法执行病毒扫描的个别或非典型的引导扇区，则应禁用引导区分析。
   - **关机时扫描软盘**。该选项为默认选项。关闭计算机时，扫描所有插在驱动器中的软盘的引导扇区。如果磁盘感染了病毒，计算机将在磁盘取出后才关闭。

4. 在 “**常规**”区域中，选择下列选项之一：

   - **在系统启动时启用按访问扫描**。该选项为默认选项。在启动计算机时启动按访问扫描服务。
   - **隔离文件夹**。接受隔离文件夹的默认位置和名称，或输入隔离文件夹的不同位置的路径，或单击 “**浏览**”在本地驱动器上查找适当的文件夹。

隔离文件夹的默认位置和名称是：

< 驱动器 >:\quarantine

注释
隔离文件夹不应位于软驱或 CD 驱动器上。它必须在硬盘上。

5 在 “**扫描时间**”区域中，以秒为单位指定所有文件的最大存档和扫描时间。如果一个文件的扫描时间超过了指定时间，扫描将干脆利落地中断，并且记录一条消息。如果扫描不能干脆利落地中断，它将终止并重新启动，同时记录一条不同的消息。从以下选项中进行选择：

- **最大存档文件扫描时间(秒)**。默认设置是15秒。接受默认设置，或输入扫描程序扫描存档文件时可以花费的最大秒数。您输入的存档扫描时间必须小于所有文件的扫描时间。
- **对所有文件执行最大扫描时间**。该选项为默认选项。对所有文件实行最大扫描时间。
- **最大扫描时间(秒)**。默认设置是45秒。接受默认设置，或输入扫描程序扫描文件时可以花费的最大秒数。

6 单击 “**应用**”保存更改。

消息属性

使用 “**消息**”选项卡上的选项，为按访问扫描配置用户消息选项。

1 打开“**按访问扫描属性**”对话框，然后选择左侧窗格中的“**常规设置**”图标。

2 选择 “**消息**”选项卡。

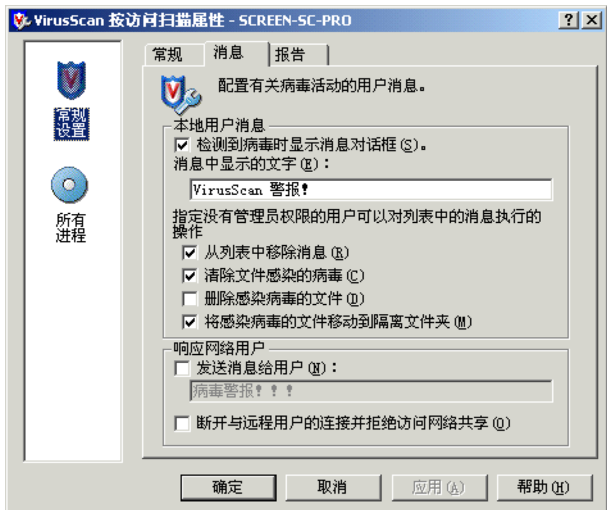


图 **3-6.** 常规设置 **-** 消息选项卡

3 在 “**本地用户消息**”区域中，选择消息选项。

以下选项适用于所有用户：

- **检测到病毒时显示消息对话框**。该选项为默认选项。检测到病毒时，显示 “**按访问扫描消息**”对话框。有关 “**按访问扫描消息**”对话框的详细信息，请参阅第 59 页的 “响应病毒检测”。

- **消息中显示的文字**。默认消息是 “VirusScan 警报 !”。如果选择了 “**检测到病毒时显示消息对话框**” ，则您可以输入检测到病毒后要显示的自定义消息。

以下选项应用于没有管理权限的用户可以对 “**按访问扫描消息**”对话框中列出的消息所进行的操作。请选择以下选项的任意组合：

- **从列表中移除消息**。该选项为默认选项。允许没有管理权限的用户移除列表中的消息。

- **清除文件感染的病毒**。该选项为默认选项。允许没有管理权限的用户清除列表中消息所提及的文件感染的病毒。

- **删除感染病毒的文件**。允许没有管理权限的用户删除列表中消息所提及的感染病毒文件。

- **将感染病毒的文件移动到隔离文件夹**。该选项为默认选项。允许没有管理权限的用户将列表中消息所提及的感染病毒文件移到隔离文件夹中。

4 在 “**响应网络用户**”区域中，从下列选项中进行选择：

- **发送消息给用户**。检测到病毒时向网络用户发送消息。例如，某个网络用户正在远程计算机上运行，并通过网络共享访问受保护的文件系统。

  如果选择了该选项，您可以在给定的文本框中输入一个自定义消息。默认消息是 “病毒警报 !!!”。

  警告
  为接收此消息，必须运行 Windows Messenger 服务。

- **断开与远程用户的连接并拒绝访问网络共享**。自动断开与那些读取您计算机上共享文件夹中感染病毒的文件或向该文件写入的用户的连接。然后，扫描程序将重写权限，以便排除试图读取共享文件夹中感染病毒的文件或向该文件写入的用户。

5 单击 “**应用**” 保存更改。

报告属性

使用 “**报告**” 选项卡上的选项来配置日志活动并为每个日志条目指定要捕获的信息。

1 打开 “**按访问扫描属性**” 对话框，然后选择左侧窗格中的 “**常规设置**” 图标。

2 选择 “**报告**” 选项卡。

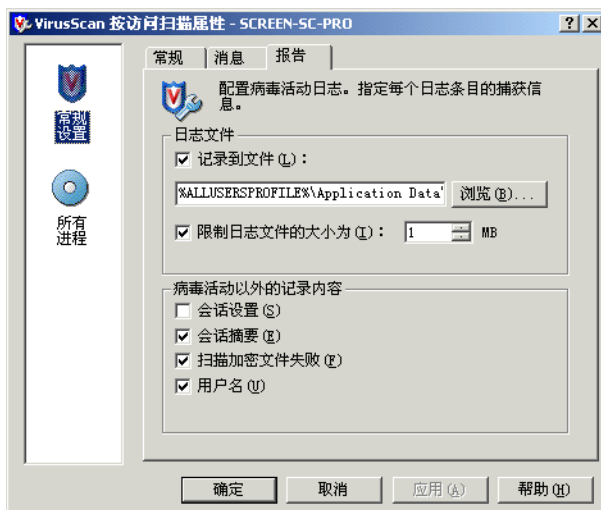


图 3-7. 常规设置 - 报告选项卡

日志文件可以作为一种重要的管理工具使用，它能够跟踪网络病毒活动、记录用来检测和响应扫描程序发现的所有病毒的设置。此外，日志文件中记录的事件报告也有助于确定需要使用备份副本替换哪些文件、在隔离文件夹中检查哪些文件或者应从计算机中删除哪些文件。以后复查时，可以从文本编辑器打开活动日志文件。

3 在 “**日志文件**”区域中，从下列选项中进行选择：

- **记录到文件**。该选项为默认选项。在日志文件中记录按访问扫描病毒活动。
- 接受文本框中默认的日志文件名称和位置，或者输入其他日志文件名称和位置，或者单击 “**浏览**”查找计算机或网络中的适当文件。

  注释
  默认情况下，扫描程序将日志信息写入如下目录中的 ONACCESSSCANLOG.TXT 文件中。

  < 驱动器 >:Winnt\Profiles\All Users\Application Data\Network Associates\Virusscan

- **限制日志文件的大小为**。该选项为默认选项。默认日志文件大小是 *1MB*。接受默认的日志大小或设置不同的日志大小。如果选择了该选项，请输入一个介于 1MB 到 999MB 之间的值。

  注释
  如果日志文件中的数据超过了您设置的文件大小，则最早的百分之二十的日志条目将被删除，接着新数据会被添加到这个文件中。

4 在 “**病毒活动以外的记录内容**”区域中，选择要记录在日志文件中的其他信息：

- **会话设置**。记录您为日志文件中每个扫描会话所选择的属性。该选项不是默认选择。

  注释
  扫描会话是指扫描程序位于计算机内存中的那段时间。当卸载该程序或者重新启动计算机时，扫描会话就会结束。

- **会话摘要**。该选项为默认选项。摘要记录扫描程序在每个扫描会话过程中执行的扫描操作，并将该信息添加到日志文件。摘要信息包括已扫描的文件数、检测到的病毒数和类型、移动、清除或删除的文件数以及其他信息。该选项为默认选择。
- **扫描加密文件失败**。该选项为默认选项。在日志文件中记录那些扫描程序无法扫描的加密文件名称。该选项为默认选择。
- **用户名**。该选项为默认选项。这样即可将记录每个日志条目时登录到计算机的用户的姓名记录在日志文件中。该选项为默认选择。

5 单击 “**应用**”保存更改。

默认、低风险和高风险进程

根据您将进程定义为低风险还是高风险，您可以灵活地设置不同的进程属性。未指定为低风险或高风险的所有进程都是默认进程。

这部分包含下列主题：

- 进程属性
- 检测属性
- 高级属性
- 操作属性

进程属性

在 “**进程**” 选项卡中，您可以为 “**默认进程**” 指定的属性可以不同于为 “**低风险进程**” 和 “**高风险进程**” 指定的属性。

- 有关 “**默认进程**” 的详细说明，请参阅 *“默认进程的进程属性”*。
- 有关“**低风险进程**”和“**高风险进程**”的详细说明，请参阅第 44 页的“低风险或高风险进程的进程属性”。

默认进程的进程属性

决定是否为所有进程设置相同属性，或者为低风险和高风险进程设置不同的属性。

1. 打开“**按访问扫描属性**”对话框，然后选择左侧窗格中的“**默认进程**”图标。
2. 选择 “**进程**” 选项卡。
3. 选择左侧窗格中的 “**所有进程**” 图标，然后选择以下选项之一：
   - **对所有进程使用这些选项卡上的设置**。该选项为默认选项。如果选择了这个选项，为 “**默认进程**” 选择的属性将应用于所有进程。此时将无法为低风险或高风险进程设置不同属性。
   - **对高风险和低风险进程使用不同的设置**。为高风险和低风险进程设置不同属性。



图 **3-8.** 默认进程 **-** 进程选项卡

4 单击 “**应用**” 保存更改。

低风险或高风险进程的进程属性

使用 “**进程**” 选项卡中的 “**添加**” 和 “**删除**” 按钮，选择哪些进程为低风险、哪些进程为高风险进程。

> **注释**
> 如果选择了 “**进程**” 选项卡中的 “**对所有进程使用这些选项卡上的设置**”，则 “**低风险进程**” 和 “**高风险进程**” 对话框将隐藏。

1 打开 “**按访问扫描属性**” 对话框，然后选择左侧窗格中的 “**低风险进程**” 图标或 “**高风险进程**” 图标。



图 **3-9.** 低风险或高风险进程 **-** 进程选项卡

2 选择 “**进程**”选项卡。

该列表按照文件名的字母顺序显示了当前进程的列表。“**低风险进程**”列表的默认设置为空。每个进程都显示了自己的应用程序图标、文件名和相关描述（如果有）。

注释

您选择低风险和高风险进程的步骤相同。

3 要添加应用程序，请单击“**添加**”。屏幕上将出现 “**选择应用程序**”对话框。



图 **3-10.** 选择应用程序

a 选择要添加的应用程序。您可以用以下方法选择应用程序：

- 从列表中选择应用程序。

  使用 CTL 和 SHIFT 键选择多个应用程序。

- 单击 “**浏览**”查找网络中的应用程序。

b 选择应用程序完毕后，单击 “**确定**”保存并返回到 “**进程**”选项卡。

4 要删除应用程序，首先突出显示列表中的一个或多个应用程序，然后单击“**删除**”。

5 单击 “**应用**”保存更改。

6 重复步骤 1 到步骤 5，为 “**低风险进程**”或 “**高风险进程**”选择应用程序。

检测属性

使用 “**检测**”选项卡，指定需要按访问扫描程序检查的文件类型和何时进行扫描。

1 打开 “**按访问扫描属性**”对话框，然后选择左侧窗格中的以下图标之一：

- **默认进程**
- **低风险进程**
- **高风险进程**

注释

如果选择了 “**进程**”选项卡中的 “**对所有进程使用这些选项卡上的设置**”，则 “**低风险进程**”和 “**高风险进程**”对话框将隐藏。

2 选择 “**检测**”选项卡。



图 **3-11.** 检测选项卡

注释

如果选择了左侧窗格中的进程图标，则设置默认进程、低风险进程和高风险进程的 “**检测**” 选项的步骤是相同的。

3 在 “**扫描文件**” 区域中，选择下列选项的任意组合：

- **写入磁盘时**。该选项为默认选项。扫描写入到服务器、工作站或其他数据存储设备、或在这些设备上进行修改的所有文件。
- **读取磁盘时**。该选项为默认选项。扫描从服务器、工作站或其他数据存储设备上读取的所有文件。
- **在网络驱动器上**。在按访问扫描过程中，扫描对象将包括网络资源。这是扩展病毒防护的一种便利方法，但是将对运行扫描的系统的总体性能产生负面影响。

警告

如果正将文件从一台计算机复制或者移到另一台计算机，并将这两台计算机上的按访问扫描属性都配置为扫描写入到磁盘的文件和从磁盘中读取的文件，因此当来源计算机读取文件时会进行扫描，而在写入到 “目标计算机” 时将再次进行扫描。

如果您网络上的主要通讯模式是将文件从一台计算机复制或移到另一台计算机，您可能希望将扫描属性配置为仅扫描写入到磁盘的文件，而不扫描从磁盘中读取的文件。这能有效防止重复扫描同一文件的情况。要获得相同结果，可将所有计算机配置为仅扫描从磁盘中读取的文件，而不扫描向磁盘写入的文件。

如果使用了这些配置之一，重要的一点就是把所有计算机配置的完全一样。切勿把某些计算机配置为仅扫描写入到磁盘的文件，而把另一些配置为扫描从磁盘读取的文件。因为这样会将感染病毒的文件从仅扫描写入到磁盘的文件的那些计算机复制到仅扫描从磁盘中读取的文件的那些计算机中。

4 在 “**扫描内容**” 区域中，选择下列选项之一：

- **所有文件**。该选项为默认选项。扫描所有文件，而不论其扩展名如何。
- **默认类型 + 其他文件类型**。扫描默认的扩展名列表以及您指定的任何其他内容。当前的 DAT 文件定义了默认的文件类型扩展名列表。您不能删除默认列表中的任何文件类型扩展名，但可以添加或删除用户指定的文件类型扩展名。同时，还可以排除默认列表中的扩展名。更多信息，请参阅第 51 页的 “排除文件、文件夹和驱动器”。
  - **其他**。如果选择了 “**默认类型 + 其他文件类型**”，请单击 “**其他**” 添加或删除用户指定的文件类型扩展名。详细说明，请参阅第 49 页的 “添加文件类型扩展名”。

    按访问扫描程序列出的最大附加扩展名的数量为 1000。
  - **同时扫描所有文件中的宏病毒**。扫描所有文件的同时检查宏病毒，而无论扩展名为何。该选项仅在选择了 “**默认类型 + 其他文件类型**” 选项后才能使用。
- **指定的文件类型**。仅扫描您指定的扩展名。
  - **指定项**。如果选择了 “**指定的文件类型**”，请单击 “**指定项**” 添加或删除用户指定的文件类型扩展名。还可以将文件类型扩展名列表设置为默认列表。详细说明，请参阅第 50 页的 “添加用户指定的文件类型扩展名”。

    按访问扫描程序可以列出的最大指定扩展名的数量为 1000。

5 在 “**不扫描内容**” 区域中，使用 “**排除**” 按钮指定不准备扫描的文件、文件夹和驱动器。详细说明，请参阅第 51 页的 “排除文件、文件夹和驱动器”。

6 单击 “**应用**” 保存更改。

7 对需要配置的每个进程类型，重复步骤 2 到步骤 6：默认、低风险或高风险。

添加文件类型扩展名

使用 “**其他**” 按钮，将用户指定的文件类型添加到文件类型默认列表中。还可以使用此功能，删除您添加的用户指定的任何文件类型。默认列表以及用户指定的文件类型都将包括在扫描范围内。

> **注释**
> 您不能更改或删除文件类型默认列表中的文件类型。默认列表由您下载的最新 DAT 文件定义。要防止扫描某个扩展名，您需要排除该扩展名。更多信息，请参阅第 51 页的 “排除文件、文件夹和驱动器”。

1. 打开 “**按访问扫描属性**” 对话框，然后选择左侧窗格中的以下图标之一：
   - **默认进程**
   - **低风险进程**
   - **高风险进程**
2. 在 “**检测**” 选项卡的 “**扫描内容**” 区域中，选择 “**默认类型 + 其他文件类型**”。
3. 单击 “**其他**” 打开 “**其他文件类型**”。

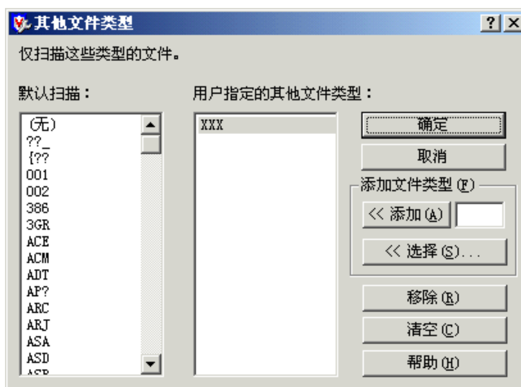


图 3-12. 其他文件类型

4. 在 “**添加文件类型**” 区域中，您可通过两种方式添加用户指定的文件类型扩展名：
   - 在文本框中输入一个文件类型扩展名，然后单击 “**添加**”。

> **注释**
> 只需输入文件类型扩展名的前三个字母。如果输入 HTM 文件扩展名，则扫描程序将扫描 HTM 和 HTML 文件。您可以使用通配符或者字符与通配符的组合。

- 单击 “**选择**” 打开 “**选择文件类型**” 对话框。从该列表中选择一个或多个文件类型扩展名，然后单击 “**确定**”。

添加的扩展名将显示在 “**用户指定的其他文件类型**” 列表中。

5 通过以下两种方法可以从用户指定的列表中删除用户指定的文件扩展名：

- 选择“**用户指定的其他文件类型**”列表中的一个或多个文件类型扩展名，然后单击 “**移除**”。
- 单击 “**清空**” 删除 “**用户指定的其他文件类型**” 列表中的所有项目。

添加用户指定的文件类型扩展名

使用 “**指定项**” 按钮创建包含在扫描范围内的用户指定的文件类型扩展名列表。还可以使用该功能删除您添加的用户指定的任何文件类型。

1 打开 “**按访问扫描属性**” 对话框，然后选择左侧窗格中的以下图标之一：

- **默认进程**
- **低风险进程**
- **高风险进程**

2 在 “**检测**” 选项卡的 “**扫描内容**” 区域中，选择 “**指定的文件类型**”。

1 单击 “**指定项**” 打开 “**指定的文件类型**” 对话框。

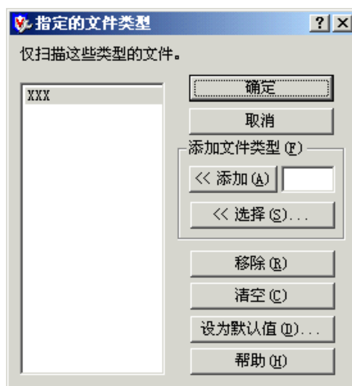


图 3-13. 指定的文件类型

2 在 “**添加文件类型**” 区域中，您可通过两种方式添加用户指定的文件类型扩展名：

- 在文本框中输入一个文件类型扩展名，然后单击 “**添加**”。

注释
只需输入文件类型扩展名的前三个字母。如果输入 HTM 文件扩展名，则扫描程序将扫描 HTM 和 HTML 文件。您可以使用通配符或者字符与通配符的组合。

- 单击 “**选择**” 打开 “**选择文件类型**” 对话框。从该列表中选择一个或多个文件类型扩展名，然后单击 “**确定**”。

添加的扩展名将显示在 “**仅扫描这些类型的文件**” 下面的列表中。

3 通过以下两种方法可以从该列表中删除用户指定的文件扩展名：

- 在 “**仅扫描这些类型的文件**” 下面的列表中选择一个或多个文件类型扩展名，然后单击 “**移除**”。
- 单击 “**清空**” 删除 “**仅扫描这些类型的文件**” 下面的列表中的所有项目。

4 单击 “**设为默认值**”，以便使用默认列表替换当前用户指定的文件类型扩展名列表。当前的 DAT 文件定义了默认的文件类型扩展名列表。

5 单击 “**确定**” 保存更改并返回到 “**检测**” 选项卡。

排除文件、文件夹和驱动器

使用 “**排除**” 按钮指定要从扫描操作中排除的文件、文件夹和驱动器。还可以使用此功能删除您指定的任意排除项。

1 打开 “**按访问扫描属性**” 对话框，然后选择左侧窗格中的以下图标之一：

- **默认进程**
- **低风险进程**
- **高风险进程**

2 在 “**检测**” 选项卡的 “**不扫描内容**” 区域中，单击 “**排除**” 打开 “**设置排除**” 对话框。

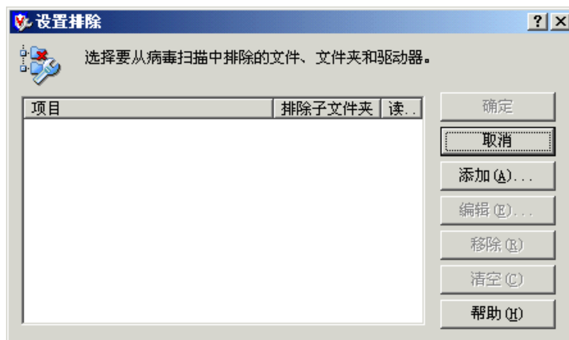


图 3-14. 设置排除

3 在“**设置排除**”对话框中，可以添加或编辑文件、文件夹或驱动器。Windows 文件保护是默认列表。

- 要添加项目，请单击 “**添加**” 打开 “**添加排除项目**” 对话框。
- 要编辑项目，请双击或选择它，然后单击 “**编辑**” 打开 “**编辑排除项目**” 对话框。

注释
排除选项都相同，且与您是添加还是编辑排除项无关。

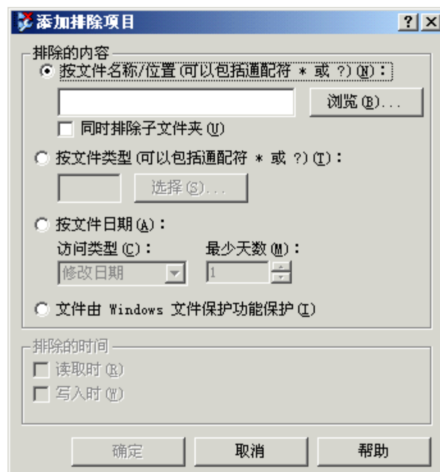


图 3-15. 添加排除项

4 在 “**排除的内容**” 区域中，选择下列选项之一：

- **按文件名称 / 位置**。该选项为默认选项。指定名称或位置。可以使用通配符 * 和 ?。在文本框中输入特定信息或单击 “**浏览**” 查找名称或位置。

  您可以指定完整的路径名 （例如 C:\WINNIT\SYSTEM*） 、完整的文件名 （例如 PAGEFILE.SYS、 PAGEFILE.*、 P*.* 或 *.SYS）或者文件夹名 （例如 BACKUP）。例如，指定 BACKUP 文件夹将不包括所有名为 BACKUP 的文件夹，且与它们的位置无关。

  - **同时排除子文件夹**。如果选择了“**按文件名称 / 位置**”，可以排除与指定格式相匹配的文件夹中的子文件夹。

- **按文件类型**。按照类型指定文件扩展名。可以使用通配符 * 和 ?。在文本框中输入文件扩展名，或者单击 “**选择**” 打开 “**选择文件类型**” 对话框，从列表中选择一个或多个扩展名。单击 “**确定**” 保存并关闭该对话框。

- **按文件日期**。指定一个文件日期。
  - **访问类型**。如果选择了 “**按文件日期**”，请单击选择一个访问类型。
  - **最少天数**。如果选择了 “**按文件日期**”，请选择一个最少天数。
- **文件由 Windows 文件保护功能保护**。指明这个排除项取决于文件的 Windows 文件保护状态。

5. 在 “**排除的时间**” 区域中，指定何时不扫描这些项目。选择以下选项的任意组合：
   - “**读取时**”。该选项为默认选项。指定从磁盘中读取时不扫描的项目。
   - “**写入时**”。该选项为默认选项。指定向磁盘写入时不扫描的项目。

   注释
   “**读取时**” 和 “**写入时**” 选项不适用于按需扫描任务。
6. 单击 “**确定**” 保存更改并返回到 “**设置排除**” 对话框。
7. 可以使用以下两种方法删除项目列表中用户指定的文件类型扩展名：
   - 从列表中选择一个或多个文件类型扩展名，然后单击 “**移除**”。
   - 单击 “**清空**” 删除列表中的所有项目。
8. 单击 “**确定**” 保存更改并返回到 “**检测**” 选项卡。
9. 单击 “**应用**” 保存更改。

高级属性

使用 “**高级**” 选项卡中的选项可以为启发式扫描、非病毒程序文件以及压缩文件指定高级扫描选项。

1. 打开 “**按访问扫描属性**” 对话框，然后选择左侧窗格中的以下图标之一：
   - **默认进程**
   - **低风险进程**
   - **高风险进程**

   注释
   如果选择了 “**进程**” 选项卡中的 “**对所有进程使用这些选项卡上的设置**”，则 “**低风险进程**” 和 “**高风险进程**” 对话框将隐藏。
2. 选择 “**高级**” 选项卡。



图 **3-16.** 高级选项卡

注释

如果选择了左侧窗格中的进程图标，则用于设置默认进程、低风险和高风险进程的 “**高级**”选项的步骤相同。

3 在“**启发式**”区域中，指定是否要求扫描程序评估一段未知代码或 Microsoft Office 宏为病毒的概率。启用该功能后，扫描程序将分析它是已知病毒的变体的可能性。请选择以下选项的任意组合：

- **查找未知程序病毒**。默认情况下，对于“**默认进程**”和“**高风险进程**”，该选项是选定的。默认情况下，对于 “**低风险进程**”， 该选项是不选定的。将含有类似病毒的代码的可执行文件作为真正感染了病毒的文件对待。扫描程序将应用您在 “**操作**”选项卡中选择的操作。

- **查找未知宏病毒**。默认情况下，对于 “**默认进程**”和 “**高风险进程**”，该选项是选定的。默认情况下，对于 “**低风险进程**”， 该选项是不选定的。将含有类似病毒的代码的嵌入式宏作为真正感染了病毒的文件对待。扫描程序将对这些文件应用您在 “**操作**”选项卡中选择的操作。

  注释

  该选项不同于 “**检测**”选项卡中的 “**同时扫描所有文件中的宏病毒**”，后面这个选项可指导扫描程序查找所有已知宏病毒。“**查找未知宏病毒**”则指导扫描程序估计未知宏是病毒的概率。

4 在 “**非病毒**”区域中，指定是否要求扫描程序查找可能有害的非病毒程序。

- **查找潜在的异常程序”**。查找潜在的异常程序，将其作为真正的染毒文件对待。

  - **“查找玩笑程序”**。如果选择了 **“查找潜在的异常程序”**，扫描程序还会扫描玩笑程序。

警告

VirusScan Enterprise 不清除可能有害的程序文件或玩笑程序。如果将扫描程序配置为 **“查找潜在的异常程序”** 和 / 或 **“查找玩笑程序”**，就不会清除检测到的任何程序或玩笑文件。

如果选定 **“自动清除文件感染的病毒”** 作为主要操作， VirusScan Enterprise 会自动执行辅助操作。如果选定 **“将感染病毒的文件移到文件夹”** 或 **“自动删除感染病毒的文件”**，则可能有合法的、已安装程序文件被移动或删除。移动或删除程序文件可能会留下注册表键、快捷方式和其他文件。

如果 VirusScan Enterprise 检测到您不想安装的可能有害的程序文件或玩笑程序，我们推荐您使用 Windows **“控制面板”** 中的 **“添加 / 删除程序”** 来完全卸载检测到的程序。您还可以联系 **“病毒信息库”**，了解有关手动卸载可能有害的程序的信息。

如果 VirusScan Enterprise 检测到您不想安装的可能有害的程序文件或玩笑程序，我们推荐您选择以下操作：

- 取消选择 **“查找潜在的异常程序”** 和 / 或 **“查找玩笑程序”** 选项。
- 排除检测到的程序文件名称。更多信息，请参阅第 51 页的“排除文件、文件夹和驱动器”。

然后，重新安装该程序文件，如果该程序文件被移动，请从隔离文件夹中恢复，如果已删除，请从备份中恢复。

5 在 **“压缩文件”** 区域中，指定扫描程序要检查的压缩文件类型。您可以选择以下选项：

- **扫描压缩文件中的可执行文件**。默认情况下，对于 **“默认进程”** 和 **“高风险进程”**。该选项是选定的。默认情况下，对于 **“低风险进程”**，该选项是不选定的。检查含有可执行文件的压缩文件。打包的可执行文件是运行时只将自己解压缩到内存中去的文件。打包的可执行文件永远不会解压缩到磁盘上。
- **扫描存档文件内部的文件**。检查存档文件及其内容。存档文件是压缩文件，要访问它包含的文件，必须首先解压缩。存档所含文件在被写入磁盘时会经过扫描。
- **解码 MIME 编码的文件**。检查 MIME 编码的文件。

注释

尽管该选项能够更好地保护用户，但扫描压缩文件还是增加了扫描所需的时间。

6 单击 “**应用**” 保存更改。

7 对需要配置的每个进程类型，重复步骤 1 到步骤 6：默认、低风险或高风险。

操作属性

使用 “**操作**” 选项卡中的选项，指定希望扫描程序在发现病毒时所执行的主要和辅助操作。

1 打开 “**按访问扫描属性**” 对话框，然后选择左侧窗格中的以下图标之一：

- **默认进程**
- **低风险进程**
- **高风险进程**

注释
如果选择了 “**进程**” 选项卡中的 “**对所有进程使用这些选项卡上的设置**”，则 “**低风险进程**” 和 “**高风险进程**” 对话框将隐藏。

2 选择 “**操作**” 选项卡。

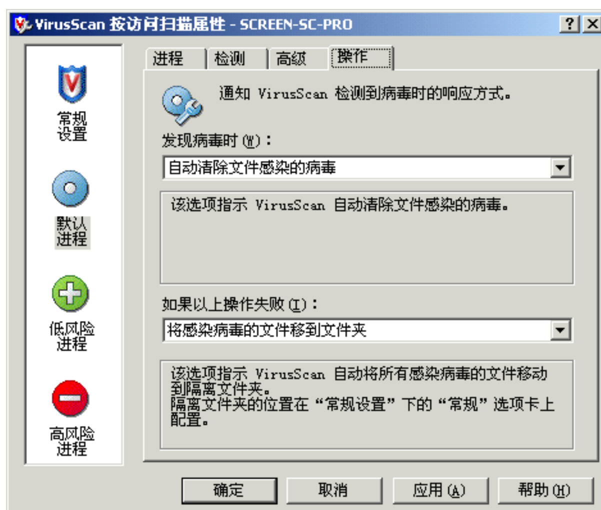


图 3-17. 操作选项卡

注释
如果选择了左侧窗格中的进程图标，则用于设置默认进程、低风险和高风险进程的 “**操作**” 选项的步骤相同。

3 在 “**发现病毒时**” 区域中，选择希望扫描程序在发现病毒时所采取的主要操作。

注释
默认的主要操作是 “**自动清除文件感染的病毒**”。

单击 ▼ 以选择如下操作之一：

- **拒绝访问感染病毒的文件**。拒绝所有用户访问扫描程序发现的任何感染病毒文件。请确保启用了 “**常规设置**” 中 “**报告**” 选项卡的 “**记录到文件**” 属性，以记录感染病毒的文件。

  执行写入操作时将添加 .VIR 扩展名，即当执行某个操作时，操作系统会认为是在向硬盘放入新的信息。如果剪切了一个文件，然后把它粘贴到同一驱动器的不同位置，则操作系统将视此操作为移动。如果文件感染了病毒，而扫描程序检测到这个感染情况，但文件名中不会被添加.VIR扩展名。

- **将感染病毒的文件移到文件夹**。默认情况下，扫描程序将感染病毒的文件移到名为 quarantine 的文件夹中。您也可以在 “**常规设置**” 中 “**常规**” 选项卡的 “**隔离文件夹**” 文本框中输入不同的文件夹名称。

- **自动删除感染病毒的文件**。当检测到病毒时，扫描程序会立即删除感染病毒的文件。请确保启用了 “**常规设置**” 中 “**报告**” 选项卡的 “**记录到文件**” 属性，以记录感染病毒的文件。

  如果选择此选项，您将被要求确认您的选择。单击 “**是**” 确认所做选择，或单击 “**否**” 取消此选项。

  警告
  如果选择了 “**高级**” 选项卡中的 “**查找未知宏病毒**”，则该操作可应用于包含类似于病毒的代码的所有宏。如果选择了 “**自动删除感染病毒的文件**”，则包含类似于宏病毒的代码的所有文件以及包含感染病毒文件的所有存档都将被删除。如果并不希望删除宏，请确保您选择的操作与您选择的宏操作一致。

- **自动清除文件感染的病毒**。该选项为默认选项。扫描程序尝试删除感染病毒文件中的病毒。如果扫描程序无法删除文件中的病毒，或如果病毒已经将文件破坏到不可修复的程度，扫描程序将执行辅助操作。更多信息，请参阅步骤 4。

4 在 “**如果以上操作失败**” 区域中，选择希望扫描程序在首选操作失败后采取何种辅助操作。具体可用的操作取决于您选择的主要操作。

   注释
   默认的辅助操作是 “**将感染病毒的文件移到文件夹**”。

5 单击 ▼ 以选择辅助操作：

   - **拒绝访问感染病毒的文件**。
   - **将感染病毒的文件移到文件夹**。该选项为默认选项。
   - **自动删除感染病毒的文件**。

     如果选择此选项，您将被要求确认您的选择。单击 “**是**” 确认所做选择，或单击 “**否**” 取消此选项。

6 单击 “**应用**”保存更改。

7 对需要配置的每个进程类型，重复步骤 1 到步骤 6：默认、低风险或高风险。

查看扫描结果

您可以在统计信息摘要和活动日志中查看按访问扫描操作的结果。

这部分包含下列主题：

- 查看扫描统计信息
- 查看活动日志

查看扫描统计信息

“**按访问扫描统计信息**”摘要显示了扫描程序已检查的文件数、找到的病毒数以及采取的响应措施。

1 打开 “**VirusScan 控制台**”。有关说明，请参阅第 18 页的 “VirusScan 控制台”。

2 应用以下方法之一，打开 “**按访问扫描统计信息**”对话框：

- 双击系统任务栏中的 。
- 右键单击任务列表中的按访问扫描任务，并选择 “**统计信息**”。



图 3-18. 按访问扫描统计信息

“**按访问扫描统计信息**”对话框在顶部窗格中显示了 “**最后扫描的文件**”，在底部窗格中显示了统计信息摘要。

3 您可以使用如下功能之一：

注释

如果显示的用户界面具有最少的菜单选项，则 “**禁用**”和 “**属性**”按钮将隐藏。该选项的设置在 “**工具**” | “**用户界面选项**” | “**显示选项**”选项卡中进行。

- 单击“**禁用**”以停止按访问扫描程序。这项功能可根据所选的操作切换。选择“**禁用**”后，这一项又会变为“**启用**”状态。要重新激活扫描程序，请单击同一对话框中的“**启用**”。
- 单击“**属性**”打开“**按访问扫描属性**”对话框，然后根据需要更改扫描属性，并单击“**应用**”保存更改。

  扫描将会立即采用新设置运行。

4. 审阅过扫描统计信息之后，单击“**关闭**”。

查看活动日志

按访问扫描活动日志显示了关于扫描操作的具体详细信息。例如，它可以显示扫描程序已检查的文件数、找到的病毒数以及采取的响应措施。

1. 打开“**VirusScan 控制台**”。有关说明，请参阅第 18 页的“VirusScan 控制台”。
2. 使用以下方法之一，打开活动日志文件：
   - 突出显示任务，然后选择“**任务**”菜单中的“**活动日志**”。
   - 右键单击任务列表中的任务，并选择“**查看日志**”。
3. 要关闭活动日志，请选择“**文件**”菜单中的“**退出**”。

响应病毒检测

按访问扫描程序根据您在“**按访问扫描属性**”对话框中选择的配置设置来查找病毒。更多信息，请参阅第 34 页的“配置按访问扫描程序”。检测到病毒后会进行以下操作：

- 如果已经将警报管理器和 / 或按访问扫描程序配置为检测到病毒后通知，您将会收到通知。
- 按访问扫描程序在“**按访问扫描消息**”对话框中记录消息。

这部分包含下列主题：

- 接收病毒检测通知
- 查看按访问扫描消息
- 检测到病毒时采取的操作

接收病毒检测通知

按访问扫描程序检测到病毒后发出的通知共有三类：

- **按访问扫描消息对话框** - “**按访问扫描消息**”对话框会显示检测到病毒的时间，但前提是您已将按访问扫描程序配置为这样做。有关配置消息选项的详细信息，请参阅第 39 页的 “消息属性”。

  有关“**按访问扫描消息**”对话框的详细信息，请参阅第 60 页的“查看按访问扫描消息”。

- **网络用户的 Messenger 服务** - 检测到病毒后向网络用户发送消息，但前提是您已经将按访问扫描程序配置为这样做。有关配置消息选项的详细信息，请参阅第 39 页的 “消息属性”。

  消息提供了关于感染病毒文件的详细信息，例如文件名、文件位置、检测到的病毒类型以及检测病毒时使用的扫描引擎版本和 DAT 文件。查看消息的详细信息，然后单击 “**确定**”取消消息。

- **Messenger 服务** - 显示网络消息，但前提是您已经将警报管理器配置为这样做。更多信息，请参阅第 118 页的 “配置警报管理器”。

  下面是警报管理器发出的网络消息的示例。



图 3-19. 按访问扫描 -Messenger 服务

消息提供了关于感染病毒文件的详细信息，例如文件名、文件位置、检测到的病毒类型以及检测病毒时使用的扫描引擎版本和 DAT 文件。查看消息的详细信息，然后单击 “**确定**”取消消息。

根据配置警报管理器和按访问扫描程序的方式，您收到的通知可能不止一个。

> **注释**
> 如果没有将三个消息选项配置为检测到病毒后发送通知，您就不会收到任何通知。但您总是能够检查 “**按访问扫描消息**”对话框来查看检测到的病毒。更多信息，请参阅第 60 页的 “查看按访问扫描消息”。

查看按访问扫描消息

检测到病毒后，按访问扫描程序在“**按访问扫描消息**”对话框中记录消息。该对话框按时间顺序为当前用户列出了所有消息。如果用户是管理员，就可以选择性地列出所有本地系统消息。

该对话框在检测到病毒后自动显示，但前提是您已经将按访问扫描程序配置为这样做。

通过右键单击系统任务栏中的 并选择 **“按访问扫描消息”**，可随时打开此对话框。

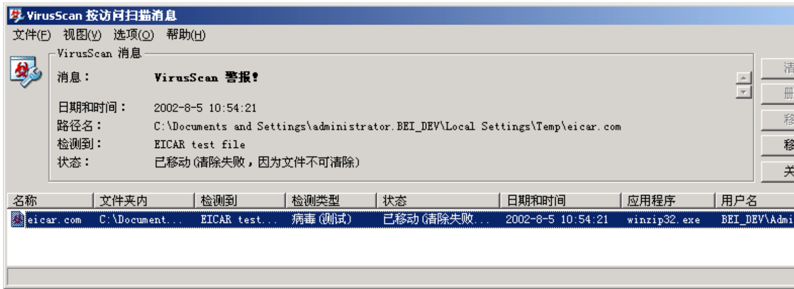


图 3-20. 按访问扫描消息

“按访问扫描消息”对话框分为几个部分：

- **菜单** - 提供了用来对文件或消息进行操作的菜单。
  - **“文件”**菜单提供了可以对列表中的文件或消息进行的操作。
  - **“视图”**菜单提供了用来控制对话框各部分可见性的选项。
  - **“选项”**菜单提供了用来显示所有消息的选项，并会使 **“按访问扫描消息”**对话框始终保持在最前。
  - **“帮助”**菜单可使您访问 VirusScan Enterprise 产品的帮助主题、访问病毒信息和技术支持网站、提交病毒样本，还可以访问关于当前安装的产品、许可、扫描引擎以及 DAT 文件的信息。
- **VirusScan 消息** - 显示了所选消息的具体信息。
- **按钮** - 显示了可用于所选消息的操作按钮。如果某个操作不能用于所选的消息，则相应的按钮将被禁用。
- **消息列表** - 列出了按访问扫描程序检测到的病毒的相关消息。可以单击列标题来为列表区域中的每一列分类。
- **状态栏** - 显示所选消息的状态。

检测到病毒时采取的操作

这部分说明了按访问扫描程序检测到病毒后您可以采取的操作。

> **注释**
> 您还可以选择向 AVERT 发送病毒样本以便进行分析。更多信息，请参阅第 31 页的 “提交病毒样本”。

通过使用 **“按访问扫描消息”**对话框，在按访问扫描程序检测到病毒后采取措施。

1 右键单击系统任务栏中的 [V]，并选择 “**按访问扫描消息**”。

2 突出显示列表中的一个消息，然后选择所需的操作。使用以下方法之一，选择操作：

   - 从 “**文件**” 菜单中。
   - 使用按钮选择操作。
   - 右键单击突出显示的消息，然后选择操作。

   可以对列表中的消息应用以下操作：

   清除文件 - 尝试清除所选消息提及的文件。

   在某些情况下，文件中的病毒可能无法清除，这可能是因为没有清除程序，也可能是因为病毒已经将文件破坏到无法修复的程度。如果无法清除文件病毒，扫描程序会在文件名后添加 .VIR 扩展名，并拒绝对该文件的访问，同时在日志文件中记录。

   注释
   如果发生这种情况，我们建议您删除此文件，并使用未感染病毒的备份副本来恢复它。

   移动文件至文件夹 - 将所选消息提及的文件移到隔离文件夹。隔离文件夹的位置在 “**按访问扫描属性**” 下 “**常规**” 选项卡中的 “**常规设置**” 中确定。

   删除文件 - 删除所选消息提及的文件。文件名将记录在日志中，以使您能够从备份副本恢复该文件。

   全选 (CTRL-A) - 选择列表中的所有消息。

   从列表中移除消息 (CTRL-D) - 从列表中删除所选的消息。从列表中删除的消息仍然可以在日志文件中看到。

   移除全部消息 - 删除列表中的所有消息。

   如果某个操作不能用于当前的消息，则相应的图标、按钮和菜单项将被禁用。例如，如果文件已删除，则 “**清除文件**” 将不可用。

   管理员可以使用 “**常规设置**” 的 “**消息**” 选项卡来配置没有管理权限的用户可以对列表中的消息执行的操作。如果管理员禁止某操作，它的按钮会隐藏，图标和菜单项也被禁用。

其他可用操作包括：

- **打开日志文件** - 打开活动日志文件。
- **关闭** - 关闭 “**按访问扫描消息**” 对话框。

按需扫描 4

按需扫描程序提供了一种在方便时或者定期扫描计算机各部分病毒的方法。它可以作为按访问扫描程序持续保护功能的一种补充，或者用来安排与您的工作不冲突的定期扫描操作。

如果只需要扫描某个文件或您认为易受攻击或怀疑包含病毒的位置，则可以执行一次性不保存的按需扫描活动，或者在方便时或定期执行预先计划的扫描活动。

这部分包含下列主题：

- 创建按需扫描任务
- 配置按需任务
- 重新设置或保存默认设置
- 计划按需任务
- 扫描操作
- 查看扫描结果
- 响应病毒检测

创建按需扫描任务

创建按需扫描任务共有三种方法。您创建的可保存或不保存的扫描类型都取决于您使用的方法。从以下选项中进行选择：

- 使用 “**开始**”菜单 - 从 “**开始**”菜单创建一次性不保存的任务。只有选择保存，该任务才能供以后使用。
- 使用系统任务栏中的 图标 - 从系统任务栏创建一次性不保存的任务。只有选择保存，该任务才能供以后使用。
- 使用“**VirusScan 控制台**”- 从控制台创建的任务都自动保存在任务列表中，以供将来使用。

这部分包含下列主题：

- 从开始菜单或系统任务栏创建任务
- 从控制台创建任务

从开始菜单或系统任务栏创建任务

从“**开始**”菜单或系统任务栏创建的按需扫描任务都是一次性不保存的任务。您可以配置、计划和运行所创建的任务，但如果不选择保存，这些任务将在关闭“**按需扫描**”属性对话框后被丢弃。

1. 打开 “**VirusScan 控制台**”。有关说明，请参阅第 18 页的 “VirusScan 控制台”。
2. 使用以下方法之一打开 “**按需扫描属性**”：
   - 单击 “**开始**”按钮，然后选择 “**程序**” | “**Network Associates**” | “**VirusScan 按需扫描**”。
   - 右键单击系统任务栏中的 并选择 “**按需扫描**”。

屏幕上将出现 “**按需扫描属性** （**未保存的任务**）” 对话框。

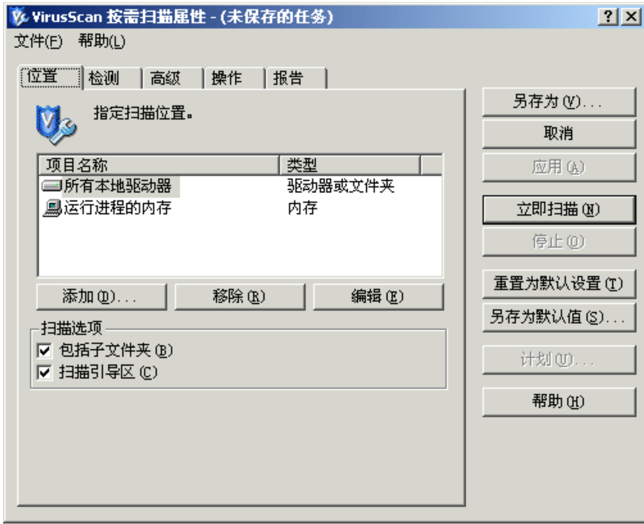


图 **4-1.** 按需扫描属性 **-** 未保存的任务

注释

您可以看出这是一个不保存的按需扫描任务，因为标题栏显示了 “**(** **未保存的任务** **)**”。要保存这个任务，请使用 “**另存为**” 按钮将任务保存到控制台，以便将来再次使用。保存任务时，“**按需扫描属性**” 标题栏从 “**(** **未保存的任务** **)**” 变为您指定的任务名。

3 配置一次性不保存的按需扫描任务。详细说明，请参阅第 67 页的 “配置按需任务”。

4 单击 “**应用**” 保存更改。

5 要计划任务，您必须首先保存任务，然后单击 “**计划**”。不能对不保存的任务进行计划。详细说明，请参阅第 176 页的 “计划任务”。

6 要运行任务，单击 “**立即扫描**”。更多信息，请参阅第 82 页的 “运行按需扫描任务”。

从控制台创建任务

“**VirusScan 控制台**”附带有默认的“**扫描所有固定磁盘**”按需扫描任务。您可以重命名该任务和 / 或创建任意多个按需扫描任务。

要从控制台创建新的扫描任务，请按照以下步骤执行：

1 打开“**VirusScan 控制台**”。有关说明，请参阅第 18 页的“VirusScan 控制台”。

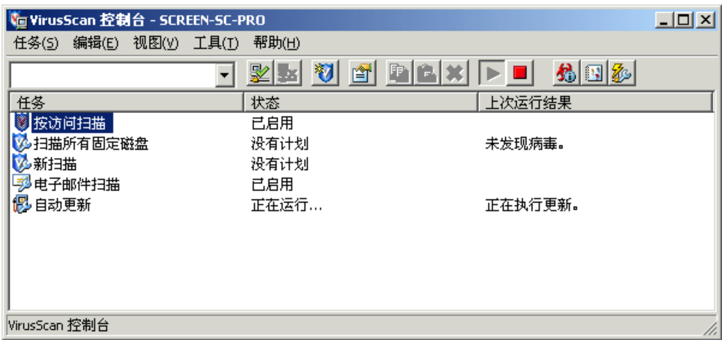


图 4-2. VirusScan 控制台

2 使用以下方法之一打开“**按需扫描属性**”：

- 无需选择任务列表中的项目，只要右键单击控制台中的空白区域，然后选择“**新建扫描任务**”。
- 选择“**任务**”菜单中的“**新建扫描任务**”。
- 单击控制台工具栏中的 。

在“**VirusScan 控制台**”任务列表中将突出显示新的按需扫描任务。

3 键入任务的新名称，然后按 ENTER 键打开 “**按需扫描属性**”对话框。

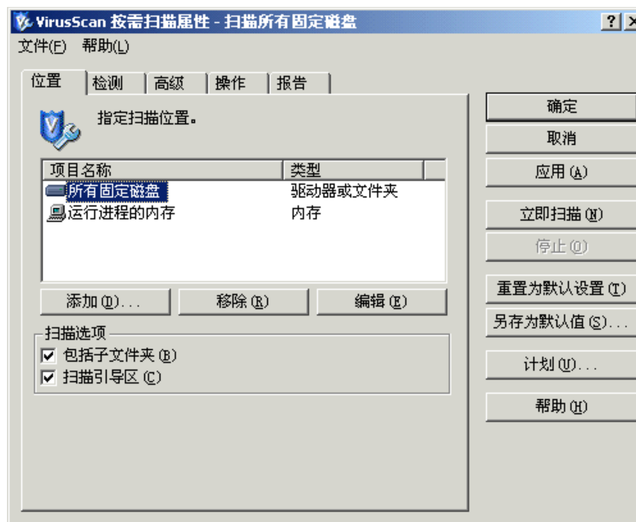


图 4-3. 按需扫描属性

配置按需任务

您可以配置按需扫描程序扫描的位置和扫描对象、在发现病毒后执行的操作以及发现病毒后如何通知您。

这部分包含下列主题：

- 位置属性
- 检测属性
- 高级属性
- 操作属性
- 报告属性
- 添加项目
- 删除项目
- 编辑项目

位置属性

使用 “**位置**”选项卡中的选项可以指定要扫描的位置。

1 为正在配置的任务打开 “**按需扫描属性**”对话框。

2 选择 “**位置**”选项卡。

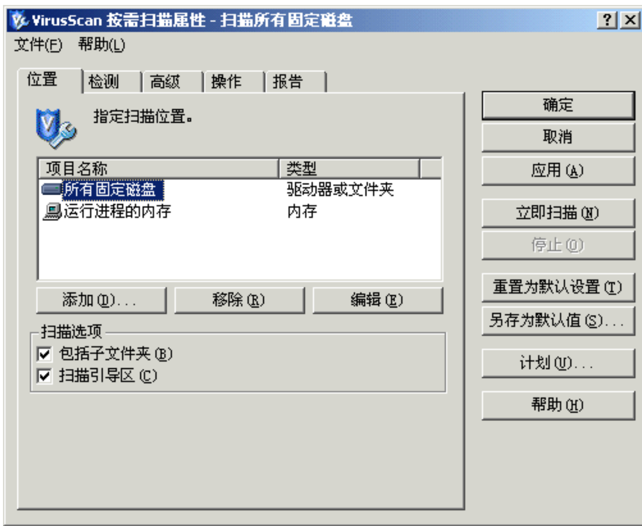


图 4-4. 按需扫描属性 - 位置选项卡

注释

默认情况下，该对话框会列出计算机上的所有驱动器以及这些驱动器包含的所有子文件夹。这种大范围的扫描操作可能会耗费较长时间。以后进行定期扫描时，您可能需要缩小扫描的范围。

3 在 “**项目名称**”区域中，指定扫描的发生位置。默认列出所有运行进程的本地驱动器和内存。使用 “**添加**”、“**移除**”和 / 或 “**编辑**”按钮指定要扫描的项目。详细说明，请参阅第 69 页的 “添加、删除和编辑项目”。

4 在 “**扫描选项**”区域中，选择扫描程序要检查计算机的哪些部分。从以下选项中进行选择：

- **包括子文件夹**。该选项为默认选项。扫描程序会检查要扫描的卷中的所有子文件夹。如果准备只扫描所选卷的根级目录，请取消选择 “**包括子文件夹**”。
- **扫描引导区**。该选项为默认选项。扫描程序检查磁盘引导扇区。如果磁盘包含无法执行病毒扫描的个别或非典型的引导扇区，则应禁用引导扇区分析。

5 单击 “**应用**”保存更改。

添加、删除和编辑项目

按照以下步骤，可以添加、删除或编辑“**按需扫描属性**”中的“**项目名称**”列表中的项目。

- 添加项目
- 删除项目
- 编辑项目

添加项目

1 为正在配置的任务打开 “**按需扫描属性**”对话框。

2 在 “**位置**”选项卡中，单击 “**添加**”打开 “**添加扫描项目**”对话框。

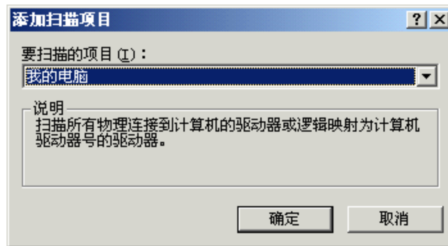


图 **4-5.** 添加扫描项目

a 单击 ▼ 从列表中选择扫描项目。可以从以下选项中进行选择：

- **我的电脑**。该选项为默认选项。扫描所有本地驱动器和映射驱动器。
- **所有本地驱动器**。扫描计算机上的所有驱动器以及它们包含的所有子文件夹。
- **所有固定磁盘**。扫描与计算机物理连接的硬盘。
- **所有可移动介质**。仅扫描软盘、光盘、 Iomega ZIP 磁盘或与计算机物理连接的类似存储设备。
- **所有网络驱动器**。扫描逻辑映射为计算机驱动器盘符的网络驱动器。
- **运行进程的内存**。扫描所有正在运行的进程的内存。该扫描在所有其他扫描之前启动。
- **用户的主文件夹**。扫描启动扫描的那个用户的主文件夹。
- **用户的配置文件文件夹**。扫描启动扫描的那个用户的配置文件。这包括 My Documents （我的文档）文件夹。
- **驱动器或文件夹**。扫描特定的驱动器或文件夹。在 “**位置**”文本框中输入驱动器或文件夹的路径，或者单击 “**浏览**”查找和选择驱动器或文件夹。

  完成浏览后，单击 “**确定**”返回到 “**添加扫描项目**”对话框。
- **文件**。扫描指定文件。在 “**位置**”文本框中输入文件路径，或单击 “**浏览**”查找和选择文件。

  完成浏览后，单击 “**确定**”返回到 “**添加扫描项目**”对话框。

b 单击 “**确定**”返回到 “**添加扫描项目**”对话框。

3 单击 “**确定**”保存更改并返回到 “**按需扫描属性**”对话框。

4 单击 “**应用**”保存更改。

删除项目

1 为正在配置的任务打开 “**按需扫描属性**”对话框。

2 在 “**位置**”选项卡中，选择 “**项目名称**”列表中要删除的一个或更多项目，然后单击 “**移除**”。

3 单击 “**是**”确认您要删除该项目。

4 单击 “**应用**”保存更改。

编辑项目

1 为正在配置的任务打开 “**按需扫描属性**”对话框。

2 在 “**位置**” 选项卡中，选择 “**项目名称**” 列表中的一项，然后单击 “**编辑**” 打开 “**编辑扫描项目**” 对话框。

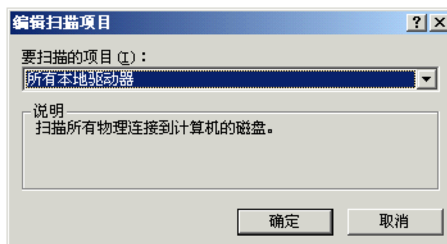


图 **4-6.** 编辑扫描项目

3 单击 ▼ 以从 “**要扫描的项目**” 列表中选择扫描项目。所有本地驱动器为默认选择。

这里的选项与 “**添加项目**” 中的选项相同。请参阅第 69 页的 “添加项目”中的步骤 a 了解完整列表以及可用选项的描述。

4 单击 “**确定**” 返回到 “**按需扫描属性**” 对话框。

5 单击 “**应用**” 保存更改。

检测属性

使用 “**检测**” 选项卡的选项指定需要按需扫描程序检查的文件类型以及何时进行扫描。

1 为正在配置的任务打开 “**按需扫描属性**” 对话框。

2 选择 “**检测**” 选项卡。

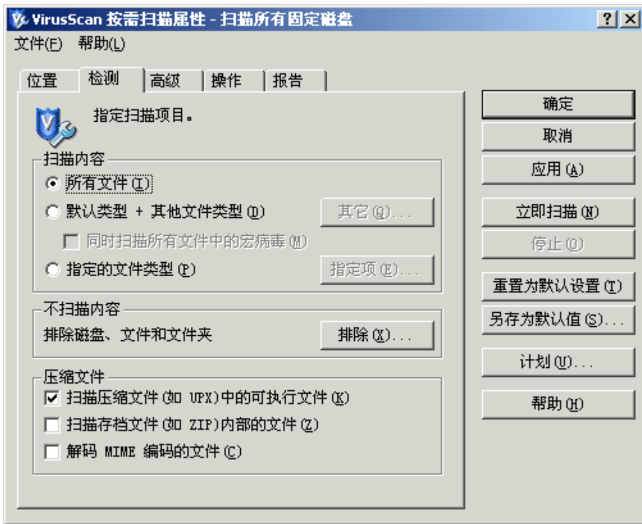


图 4-7. 按需扫描属性 - 检测选项卡

3 在 “**扫描内容**” 区域中，选择下列选项之一：

- **所有文件**。该选项为默认选项。扫描所有文件，而不论其扩展名如何。
- **默认类型 + 其他文件类型**。扫描默认的扩展名列表以及您指定的任何其他内容。当前的 DAT 文件定义了默认的文件类型扩展名列表。您不能删除默认列表中的任何文件类型扩展名，但可以添加或删除用户指定的文件类型扩展名。同时，还可以排除默认列表中的扩展名。更多信息，请参阅第 51 页的 “排除文件、文件夹和驱动器”。
  - **其他**。如果选择了 “**默认类型 + 其他文件类型**”，请单击 “**其它**” 添加或删除用户指定的文件类型扩展名。详细说明，请参阅第 49 页的 “添加文件类型扩展名”。

    按需扫描程序列出的其他扩展名的最大数量为 1000。
  - **同时扫描所有文件中的宏病毒**。扫描所有文件的同时检查宏病毒，而无论扩展名为何。该选项仅在选择了 “**默认类型 + 其他文件类型**” 选项后才能使用。
- **指定的文件类型**。仅扫描您指定的扩展名。
  - **指定项**。如果选择了 “**指定的文件类型**”，请单击 “**指定项**” 添加或删除用户指定的文件类型扩展名。还可以将文件类型扩展名列表设置为默认列表。详细说明，请参阅第 50 页的 “添加用户指定的文件类型扩展名”。

    按需扫描程序列出的指定扩展名的最大数量为 1,000。

4 在 “**不扫描内容**”区域中，使用 “**排除**”按钮指定不扫描的文件、文件夹和驱动器。详细说明，请参阅第 51 页的 “排除文件、文件夹和驱动器”。

5 在 “**压缩文件**”区域中，指定扫描程序要检查的压缩文件类型。您可以选择以下选项：

- **扫描压缩文件中的可执行文件**。该选项为默认选项。检查含有可执行文件的压缩文件。打包的可执行文件是运行时只将自己解压缩到内存中去的文件。打包的可执行文件永远不会解压缩到磁盘上。
- **扫描存档文件内部的文件**。检查存档文件及其内容。存档文件是压缩文件，要访问它包含的文件，必须首先解压缩。存档所含文件在被写入磁盘时会经过扫描。
- **解码 MIME 编码的文件**。检查 MIME 编码的文件。

6 单击 “**应用**”保存更改。

高级属性

使用“**高级**”选项卡的选项可以指定高级扫描属性，例如扫描未知程序病毒和可能有害的程序、设置 CPU 使用率和杂项。

1 为正在配置的任务打开 “**按需扫描属性**”对话框。

2 选择 “**高级**”选项卡。

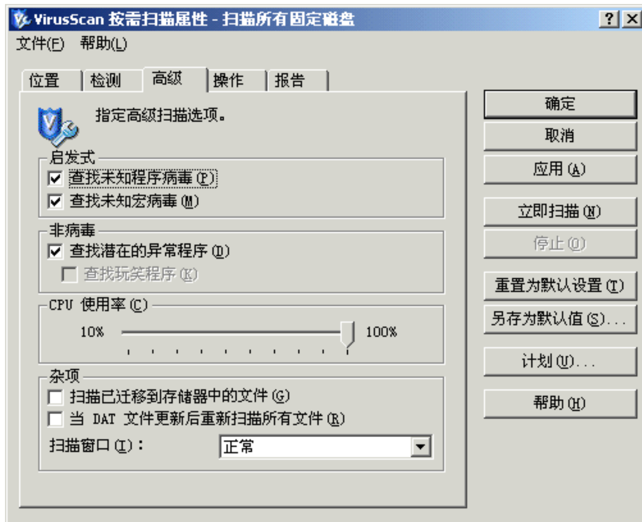


图 **4-8.** 按需扫描属性 **-** 高级选项卡

3 在“**启发式**”区域中，指定是否要求扫描程序评估一段未知代码或 Microsoft Office 宏为病毒的概率。启用该功能后，扫描程序将分析它是已知病毒的变体的可能性。请选择以下选项的任意组合：

- **查找未知程序病毒**。该选项为默认选项。将含有类似病毒的代码的可执行文件作为真正感染了病毒的文件对待。扫描程序将应用您在 “**操作**”选项卡中选择的操作。
- **查找未知宏病毒**。该选项为默认选项。将含有类似病毒的代码的嵌入式宏作为真正感染了病毒的文件对待。扫描程序将对这些文件应用您在“**操作**”选项卡中选择的操作。

注释
该选项不同于 “**检测**”选项卡中的 “**同时扫描所有文件中的宏病毒**”，后面这个选项可指导扫描程序查找所有已知宏病毒。“**查找未知宏病毒**”则指导扫描程序估计未知宏是病毒的概率。

4 在 “**非病毒**”区域中，指定是否要求扫描程序查找可能有害的非病毒程序。

- **查找潜在的异常程序**。查找潜在的异常程序，将其作为真正的染毒文件对待。
  - **查找玩笑程序**。如果选择了 “**查找潜在的异常程序**”， 则您还会扫描可能有害的玩笑程序。

警告
VirusScan Enterprise 不清除可能有害的程序文件或玩笑程序。如果将扫描程序配置为 “**查找潜在的异常程序**”和 / 或 “**查找玩笑程序**”，就不会清除检测到的任何程序或玩笑文件。

如果选定 “**清除文件感染的病毒**”作为主要操作， VirusScan Enterprise 会自动执行辅助操作。如果选定 “**将感染病毒的文件移到文件夹**”或 “**删除感染病毒的文件**”，则可能有合法的、已安装程序文件被移动或删除。移动或删除程序文件可能会留下注册表键、快捷方式和其他文件。

如果 VirusScan Enterprise 检测到您不想安装的可能有害的程序文件或玩笑程序，我们推荐您使用 Windows “**控制面板**”中的 “**添加 / 删除程序**”来完全卸载检测到的程序。您还可以联系 “**病毒信息库**”，了解有关手动卸载可能有害的程序的信息。

如果 VirusScan Enterprise 检测到您不想安装的可能有害的程序文件或玩笑程序，我们推荐您选择以下操作：

- 取消选择 “**查找潜在的异常程序**”和 / 或 “**查找玩笑程序**”选项。
- 排除检测到的程序文件名称。更多信息，请参阅第 51 页的“排除文件、文件夹和驱动器”。

然后，重新安装该程序文件，如果该程序文件被移动，请从隔离文件夹中恢复，如果已删除，请从备份中恢复。

5 在 “**CPU 使用率**”区域中，拖动滑块来设置与计算机上正在运行的其他任务相比的扫描任务的 CPU 使用率。90% 为默认选择。这确保了其他软件的运行速度在扫描过程中不受影响，但是扫描需要的时间更长。如果您计划在 CPU 运行其他必要操作（即 CPU 负载较高）的同时运行扫描任务，就需要降低扫描任务的使用率。

注释
您指定的 CPU 限制在扫描加密文件时无效。加密通过 LSASS.EXE 而不是 SCAN32 处理完成。扫描加密文件需要大量占用 CPU，因此即使 CPU 扫描线程限制非常低，它仍然以足够快的速度扫描文件， LSASS.EXE 必须保持高负载以提供加密数据。

6 在 “**杂项**”区域中，选择下列选项之一：

- **扫描已迁移到存储器中的文件**。扫描已迁移到离线存储设备中的文件。

  注释
  如果正在使用 Remote Storage 扩展服务器的磁盘空间，则按需扫描程序可以扫描高速缓存中的文件。

  Remote Storage 数据存储是分层的，具有两个规定的级别。高级称为本地存储器，包括正在 Windows 2000 服务器上运行 Remote Storage 的计算机的 NTFS 磁盘卷。低级称为远程存储器，位于连接到服务器计算机的自动磁带库或独立磁带驱动器上。

  Remote Storage 会将本地卷中符合条件的文件自动复制到磁带库中，然后监控本地卷上的可用空间。文件数据都经过本地高速缓存，因此您可以在需要时快速使用这些数据。如果必要， Remote Storage 可以将数据从本地存储器移到远程存储器中。要访问存储在由 Remote Storage 管理的卷上的文件，只需正常打开文件即可。如果文件数据不再经过本地卷缓存， Remote Storage 将从磁带库重新调用该数据。

- **当 DAT 文件更新后重新扫描所有文件**。该选项为默认选项。当新的 DAT 文件安装或更新后，请重新检查所有文件。此功能最适用于可恢复的计划扫描任务。该功能可以针对新病毒重新检查文件，从而减少感染病毒的风险。

- **扫描窗口**。正常为默认选择。单击 ▼ 以指定扫描窗口在按需扫描过程中显示的方式。选项包括：

  - **正常**
  - **最小化**
  - **隐藏**

  注释
  尽管您可以将扫描窗口配置为正常、最小化或隐藏，计划任务窗口和远程任务窗口却始终隐藏，而不论配置模式如何。

7 单击 “**应用**”保存更改。

操作属性

使用“**操作**”选项卡中的选项，指定希望扫描程序在发现病毒时所执行的主要和辅助操作。

1 为正在配置的任务打开 “**按需扫描属性**”对话框。

2 选择 “**操作**”选项卡。

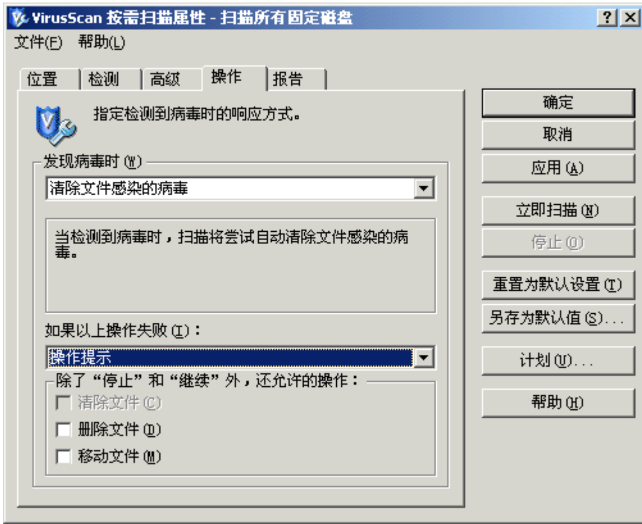


图 4-9. 按需扫描属性 - 操作选项卡

3 在 “**发现病毒时**”区域中，选择希望扫描程序在发现病毒时所采取的主要操作。

注释
默认的主要操作是 “**清除文件感染的病毒**”。

单击 ▼ 以选择如下操作之一：

- **操作提示**。提示用户在检测到病毒时采取何种操作。

  如果选择了这个选项，您还可以选择除 “**停止**”和 “**继续**”以外的操作。其他选择包括：

  - **清除文件**。允许清除文件感染的病毒。
  - **删除文件**。允许删除感染病毒的文件。
  - **移动文件**。允许移动感染病毒的文件。

  该选项不允许使用辅助操作。

- **继续扫描**。在发现感染病毒的文件后继续扫描。

  该选项不允许使用辅助操作。

  “将感染病毒的文件移到文件夹” 。扫描程序将感染病毒的文件移到 quarantine 文件夹中。您可以接受 **“文件夹”**文本框中的默认文件夹位置，也可以单击 **“浏览”**找到文件夹所在的位置。

  隔离文件夹的默认位置和名称是：

  < 驱动器 >:\quarantine

  注释
  隔离文件夹不应位于软驱或 CD 驱动器上。它必须在硬盘上。

- **清除文件感染的病毒**。该选项为默认选项。扫描程序尝试删除感染病毒文件中的病毒。如果扫描程序无法删除文件中的病毒，或如果病毒已经将文件破坏到不可修复的程度，扫描程序将执行辅助操作。更多信息，请参阅步骤 4。

- **删除感染病毒的文件**。当检测到病毒时，扫描程序会立即删除感染病毒的文件。请确保启用了 **“报告”**选项卡中的 **“记录到文件”**属性，以记录那些被感染的文件。

  如果选择此选项，您将被要求确认您的选择。单击 **“是”**确认所做选择，或单击 **“否”**取消此选项。

  警告
  如果选择了 **“高级”**选项卡中的 **“查找未知宏病毒”**，则该操作可应用于包含类似于病毒的代码的所有宏。如果选择了 **“删除感染病毒的文件”**，则包含类似于宏病毒的代码的所有文件以及包含感染病毒文件的所有存档都将被删除。如果并不希望删除宏，请确保您选择的操作与您选择的宏操作一致。

4 在 **“如果以上操作失败”**区域中，选择希望扫描程序在首选操作失败后采取何种辅助操作。

  注释
  默认的辅助操作是 **“将感染病毒的文件移到文件夹”**。

  单击 ▼ 以选择如下操作之一：

  - **操作提示**。如果选择了这个选项，您还可以选择除 **“停止”**和 **“继续”**以外的操作。其他选择包括：

    - **清除文件**。允许清除文件感染的病毒。如果已选择 **“清除文件感染的病毒”**为主要操作，则该选项被禁用。
    - **删除文件**。允许删除感染病毒的文件。如果已选择 **“删除感染病毒的文件”**为主要操作，则该选项被禁用。
    - **移动文件**。允许移动感染病毒的文件。如果已选择 **“移动感染病毒的文件”**为主要操作，则该选项被禁用。

- **继续扫描**。在发现感染病毒的文件后继续扫描。
- **将感染病毒的文件移到文件夹**。该选项为默认选项。扫描程序将感染病毒的文件移到 quarantine 文件夹中。您可以接受 “**文件夹**” 文本框中的默认文件夹位置，也可以单击 “**浏览**” 找到文件夹所在的位置。

  隔离文件夹的默认位置和名称是：

  < 驱动器 >:\quarantine

  注释
  隔离文件夹不应位于软驱或 CD 驱动器上。它必须在硬盘上。

- **删除感染病毒的文件**。当检测到病毒时，扫描程序会立即删除感染病毒的文件。请确保启用了 “**报告**” 选项卡中的 “**记录到文件**” 属性，以记录那些被感染的文件。

5 单击 “**应用**” 保存更改。

报告属性

使用“**报告**”选项卡上的选项配置记录活动。指定日志文件的位置和大小以及每个日志项要捕捉的信息。

1 打开“**按需扫描属性**”对话框。

2 选择“**报告**”选项卡。

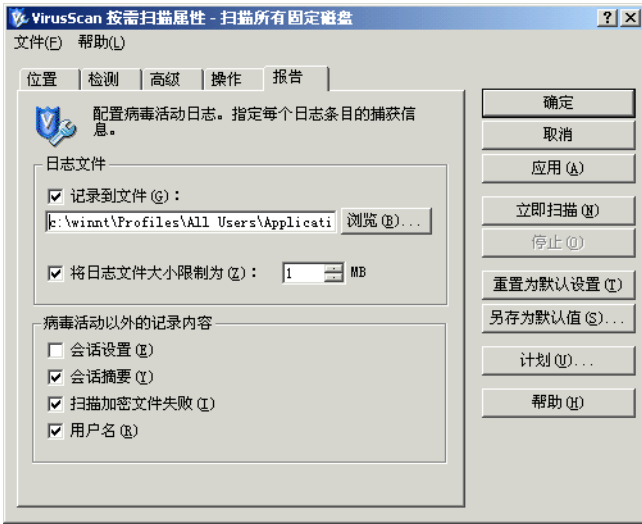


图 4-10. 按需扫描属性 - 报告选项卡

活动日志文件可以作为一种重要的管理工具使用，它能够跟踪网络病毒活动、记录用来检测和响应扫描程序发现的所有病毒的设置。以后复查时，可以从文本编辑器打开活动日志文件。此外，日志文件中记录的事件报告也有助于确定需要使用备份副本替换哪些文件、在隔离文件夹中检查哪些文件或者应从计算机中删除哪些文件。

3 在“**日志文件**”区域中，从下列选项中进行选择：

- **记录到文件**。该选项为默认选项。在日志文件中记录按需扫描病毒活动。
- 接受文本框中默认的日志文件名称和位置，或者输入其他日志文件名称和位置，或者单击“**浏览**”查找计算机或网络中的适当文件。

注释

默认情况下，扫描程序将日志信息写入如下目录中的 ONDEMANDSCANLOG.TXT 文件中。

< 驱动器 >:Winnit\Profiles\All Users\Application Data\Network Associates\Virusscan

- **将日志文件大小限制为**。该选项为默认选项。默认日志文件大小是 1MB。接受默认的日志大小或设置不同的日志大小。如果选择了该选项，请输入一个介于 1MB 到 999MB 之间的值。

  注释
  如果日志文件中的数据超过了您设置的文件大小，则最早的百分之二十的日志条目将被删除，接着新数据会被添加到这个文件中。

4 在 “**病毒活动以外的记录内容**”区域中，选择要记录在日志文件中的其他信息：

- **会话设置**。记录您为日志文件中每个扫描会话所选择的属性。该选项不是默认选择。
- **会话摘要**。该选项为默认选项。摘要记录扫描程序在每个扫描会话过程中执行的扫描操作，并将该信息添加到日志文件。摘要信息包括已扫描的文件数、检测到的病毒数和类型、移动、清除或删除的文件数以及其他信息。该选项为默认选择。
- **扫描加密文件失败**。该选项为默认选项。在日志文件中记录那些扫描程序无法扫描的加密文件名称。该选项为默认选择。
- **用户名**。该选项为默认选项。这样即可将记录每个日志条目时登录到计算机的用户的姓名记录在日志文件中。该选项为默认选择。

5 单击 “**应用**”保存更改。

重新设置或保存默认设置

在配置完按需扫描任务之后，您可以选择将配置设置重新设置为默认设置，也可以将当前配置设置保存为默认设置。

如果不希望重新设置默认设置或将当前设置保存为默认设置，请跳过这几步。

1 从以下选项中进行选择：

- **重置为默认设置**。恢复默认的扫描设置。
- **另存为默认值**。将当前的扫描配置保存为默认配置。如果选择了 “**另存为默认值**”，则所有新任务都按照这个配置创建。

2 单击 “**应用**”保存更改。

计划按需任务

配置完按需扫描任务之后，可以安排这个任务在特定的日期和时间运行，或者每隔一段时间运行一次。

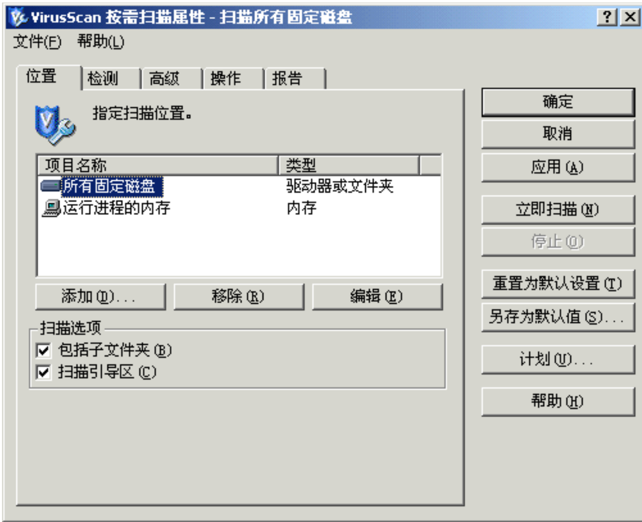


图 4-11. 按需扫描属性 - 计划

1 为正在配置的任务打开 “**按需扫描属性**” 对话框。

2 单击“**计划**”。请参阅第 175 页的“计划任务”了解如何计划任务的详细说明。

扫描操作

您可以在无人值守的情况下运行事先计划的按需扫描任务、直接启动扫描任务，也可以在扫描操作过程中暂停、停止和重新启动任务。

注释
在扫描操作中，按需扫描任务不扫描它自有的 quarantine 文件夹。设计按需扫描程序时就将 quarantine 文件夹排除在扫描范围之外，以避免重复扫描或循环扫描。

这部分包含下列主题：

- 运行按需扫描任务
- 暂停和重新启动按需扫描任务
- 停止按需扫描任务

- 可恢复的扫描

运行按需扫描任务

一旦使用所需的扫描属性配置了您的任务，就可以使用以下方法之一运行扫描任务：

- **按计划扫描**。如果计划了扫描任务，则任务可以在无人值守的情况下运行。

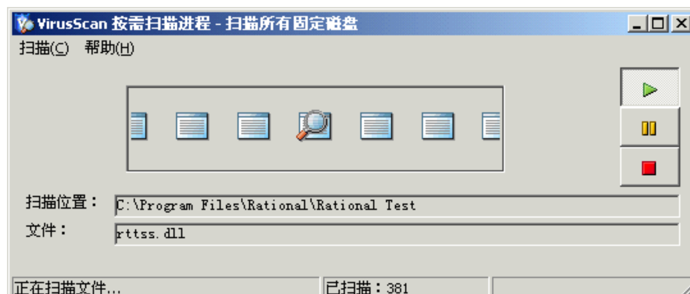


图 4-12. 按需扫描任务 - 进程中

注释
要使扫描程序运行您的任务，计算机必须处于活动状态。如果系统在计划任务开始运行时处于关机状态，那么这项任务将在计算机处于开机状态时的下一个计划时间运行，或者，如果选择了 “**计划**”选项卡中 “**计划设置**”的 “**运行错过的任务**”选项，这项任务将在计算机启动时开始。

注释
扫描程序总是在执行完由计划程序启动的计划任务以及远程计算机上运行的远程任务之后退出。

- **立即扫描**。立即启动按需扫描任务的方法有多种：
  - 从系统任务栏或 “**开始**”菜单创建按需扫描任务，然后在 “**按需扫描属性**”对话框中单击 “**立即扫描**”。
  - 在 “**VirusScan 控制台**”中，右键单击按需扫描任务并选择 “**启动**”。
  - 在 Windows 资源管理器中右键单击一个项目，然后选择 “**扫描病毒**”。

  屏幕上将出现 “**按需扫描**”对话框。



图 **4-13.** 按需扫描 - 进程中

注释
扫描程序不会在执行完这几种直接扫描后自动退出。要退出扫描程序，请选择 “**扫描**”菜单中的 “**退出**”。

暂停和重新启动按需扫描任务

您可以在扫描操作过程中暂停和重新启动按需扫描任务。

- 要暂停按需任务，请单击 “**按需扫描**”对话框中的 。
- 要重新启动按需任务，请单击 “**按需扫描**”对话框中的 。

停止按需扫描任务

按照以下方法之一，在扫描操作过程中停止按需扫描任务：

- 单击 “**按需扫描**”对话框中的 。
- 在 “**按需扫描属性**”对话框中单击 “**停止**”。

可恢复的扫描

按需扫描程序能够从上次扫描中断处自动恢复运行。按需扫描程序的增量扫描功能能够识别它扫描的最后一个文件，因此下次启动扫描时，您可以选择从中断处开始扫描，或者从头开始扫描。

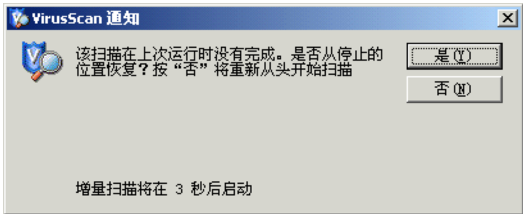


图 **4-14.** 可恢复的扫描

查看扫描结果

您可以在统计信息摘要和活动日志中查看按需扫描操作的结果。

这部分包含下列主题：

- 查看扫描统计信息
- 查看活动日志

查看扫描统计信息

“**按需扫描统计信息**”摘要显示了扫描程序已检查的文件数、找到的病毒数以及采取的响应措施。

要查看任务的统计信息和结果，请执行如下步骤：

1 打开“**VirusScan 控制台**”，右键单击任务列表中的按需扫描任务，然后选择“**统计信息**”。

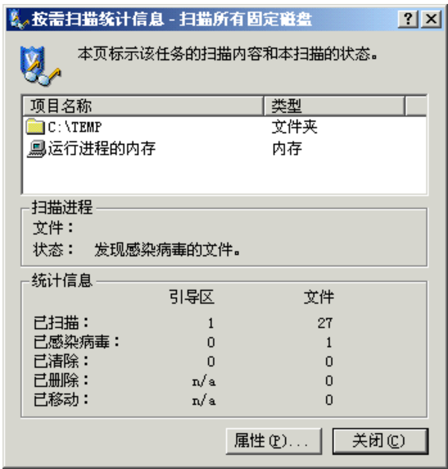


图 **4-15.** 按需扫描统计信息

“**按需扫描统计信息**”对话框在顶部窗格中显示了为该任务选定的所有扫描目标，在中部窗格中显示了扫描进程，而在底部窗格中显示了统计信息摘要。

当扫描任务运行时，扫描程序正在检查的文件和扫描操作的状态将显示在中部窗格中。

注释

该任务再次运行时，底部窗格将显示上次扫描的统计信息。

2 单击 “**属性**”打开 “**按需扫描属性**”对话框并根据需要更改扫描属性，然后单击 “**应用**”保存更改。

下次启动按需扫描时，扫描任务将使用新的设置运行。如果更改扫描属性时正在执行某个按需扫描，则直到下次启动按需扫描时，新设置才会生效。

3 审阅过扫描统计信息之后，单击 “**关闭**”。

查看活动日志

按需扫描活动日志显示了关于扫描操作的详细信息。例如，它可以显示扫描程序已检查的文件数、找到的病毒数以及采取的响应措施。

1 打开 “**VirusScan 控制台**”。有关说明，请参阅第 18 页的 “VirusScan 控制台”。

2 使用以下方法之一，打开活动日志文件：

- 突出显示任务，然后选择 “**任务**”菜单中的 “**活动日志**”。
- 右键单击任务列表中的任务，并选择 “**查看日志**”。

3 要关闭活动日志，请选择 “**文件**”菜单中的 “**退出**”。

响应病毒检测

按需扫描程序根据您在 “**按需扫描属性**”对话框中选择的配置设置来查找病毒。更多信息，请参阅第 67 页的 “配置按需任务”。

如果警报管理器和 / 或按需扫描程序已被配置为检测到病毒后通知，则您将在检测到病毒后收到通知。

这部分包含下列主题：

- 接收病毒检测通知
- 采取病毒检测操作

接收病毒检测通知

按需扫描程序检测到病毒后发出的通知共有三类：

- **VirusScan 警报** - 如果您已经在 “**操作**”选项卡中将 “**提示操作**”配置为按需扫描程序的主要或辅助操作，则检测到病毒后屏幕上将显示一个警报对话框。更多信息，请参阅第 76 页的 “操作属性”。

  有关 “**VirusScan 警报**”的详细说明，请参阅第 86 页的 “采取病毒检测操作”。

- **Messenger 服务** - 显示网络消息，但前提是您已经将警报管理器配置为这样做。更多信息，请参阅第 118 页的 “配置警报管理器”。

下面是警报管理器发出的网络消息的示例：



图 4-16. 按需扫描 - Messenger 服务

消息提供了关于感染病毒文件的详细信息，例如文件名、文件位置、检测到的病毒类型以及检测病毒时使用的扫描引擎版本和 DAT 文件。查看消息的详细信息，然后单击 “**确定**” 取消消息。

- **按需扫描进程对话框** - 当按需扫描程序正在执行任务时，屏幕上会显示“**按需扫描进程**”对话框。一旦发现病毒感染情况，它们将显示在该对话框的底部窗格中。更多信息，请参阅第 86 页的 “采取病毒检测操作”。

根据配置警报管理器和按需扫描程序的方式，您收到的通知可能不止一个。

> **注释**
> 如果未配置警报管理器或按需扫描程序这样做，您就不会收到“**VirusScan 警报**”或网络消息。但在扫描操作过程中，您总是能够从“**按需扫描消息**”对话框中查看检测到的病毒。

采取病毒检测操作

这部分说明了按需扫描程序检测到病毒后您可以采取的操作。

> **注释**
> 您还可以选择向 AVERT 发送病毒样本以便进行分析。更多信息，请参阅第 31 页的 “提交病毒样本”。

根据您的病毒检测通知方式，使用 “**VirusScan 警报**”对话框或 “**按需扫描进程**”对话框处理检测到的病毒。

- 当通知方式为“**VirusScan 警报**”时，您需要通过该对话框对病毒进行操作。
- 如果从 “**按需扫描进程**”对话框查看病毒检测，则从这里进行操作。

VirusScan 警报对话框

“**VirusScan 警报**”对话框将显示在屏幕上，通知您病毒检测结果，但前提是您已经将按需扫描程序配置为这样做。该对话框将提供检测到的感染病毒文件的位置和病毒类型的相关信息。

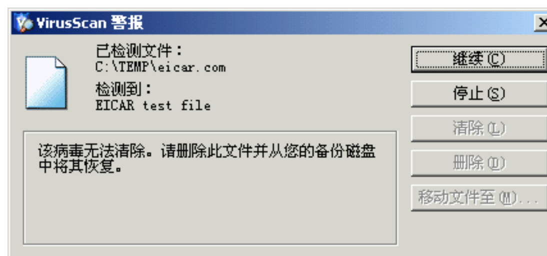


图 4-17. VirusScan 警报

选择要对感染病毒的文件执行的操作：

- **继续** - 继续扫描操作、记录活动中的每项检测以及在“**按需扫描**”窗口中列出感染病毒的所有文件。
- **停止** - 立即停止扫描操作。
- **清除** - 尝试清除所选消息提及的文件所感染的病毒。

  如果无法清除文件的病毒，可能是因为没有清除程序，也可能是因为文件已被病毒破坏到无法修复的程度，扫描程序会在日志文件中加以记录，同时可能为您提供可选的响应方法。如果无法清除文件的病毒，您应删除此文件，并用未感染病毒的备份副本恢复它。
- **删除** - 删除所选消息提及的文件。文件名将记录在日志中，以使您能够从备份副本恢复该文件。
- **移动文件至** - 将所选消息提及的文件移到在选择此按钮之后显示的对话框中选择的文件夹。

按需扫描进程对话框

当按需扫描程序执行任务时，屏幕上会显示“**按需扫描进程**”对话框。底部窗格为您列出了按需扫描检测到的病毒。



图 **4-18.** 按需扫描进程 **-** 检测到的病毒

1. 使用以下方法之一处理检测到的病毒：
   - 右键单击底部窗格中的名称，并从菜单中选择要执行的操作。
   - 突出显示底部窗格中的名称，并从 “**扫描**”菜单中选择要执行的操作。
2. 对列表中的所有感染病毒文件都执行完操作之后，选择“**扫描**”菜单中的“**退出**”关闭该对话框。

电子邮件扫描 5

电子邮件扫描程序允许您采用两种方法扫描本地主机或远程主机上的电子邮件文件夹、附件和邮件正文：

- 如果 Microsoft Outlook 正在运行，按发送电子邮件扫描程序将在发送邮件时检查电子邮件及其附件。您可以从“**VirusScan 控制台**”配置和运行按发送电子邮件扫描程序。
- 按需电子邮件扫描程序将根据需要从 Microsoft Outlook 检查电子邮件及其附件。您可以从 Microsoft Outlook 中配置和运行按需电子邮件扫描程序。

  按需电子邮件扫描程序是按发送电子邮件扫描程序防护功能的补充。如果关闭了 Microsoft Outlook 或是初次安装 VirusScan Enterprise 产品，我们建议您首先运行按需电子邮件扫描。您可以从 Microsoft Outlook 中配置和运行按需电子邮件扫描程序。

这部分包含下列主题：

- 按发送电子邮件扫描
- 按需电子邮件扫描

按发送电子邮件扫描

按发送电子邮件扫描程序将在通过 Microsoft Outlook 发送邮件时扫描电子邮件附件和邮件正文。

警告
当 Microsoft Outlook 离线时，按发送扫描程序不扫描入站的电子邮件消息。如果您的 Microsoft Outlook 离线，我们建议一旦启动 Outlook，就立即运行按需电子邮件扫描。详细说明，请参阅第 103 页的 “按需电子邮件扫描”。

这部分包含下列主题：

- 配置按发送电子邮件任务
- 查看按发送电子邮件扫描结果

配置按发送电子邮件任务

“**VirusScan 控制台**”附带有默认的按发送 “**电子邮件扫描**”，您也可以对它进行配置以满足需要。您可以通过本地或远程主机上的“**VirusScan 控制台**”配置“**电子邮件扫描**”。

要配置按发送任务，请按以下步骤操作：

1 打开 “**VirusScan 控制台**”。有关说明，请参阅第 18 页的 “VirusScan 控制台”。

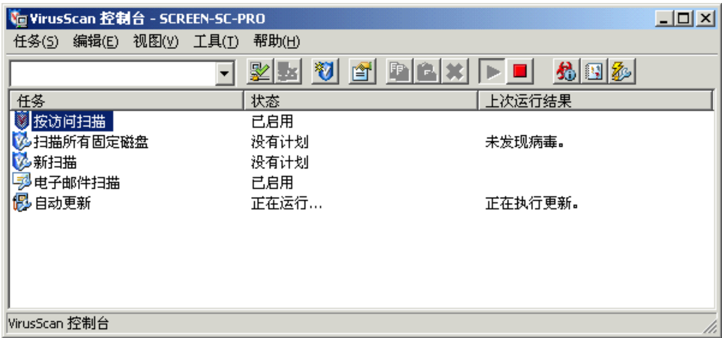


图 5-1. VirusScan 控制台

如果正在配置本地主机的 “**电子邮件扫描**”，请跳过步骤 2 并转到步骤 3。

2 如果正在配置远程主机的 “**电子邮件扫描**”：

   a 从 “**工具**”菜单中，选择 “**远程连接**”。

   b 输入计算机名称或单击 “**浏览**”查找计算机。

   c 单击 “**确定**”返回到 “**VirusScan 控制台**”。

3 使用以下方法之一，打开 “**按需扫描属性**”对话框：

   - 突出显示任务列表中的 “**电子邮件扫描**”，然后单击 。
   - 右键单击任务列表中的 “**电子邮件扫描**”，然后选择 “**属性**”。
   - 双击任务列表中的 “**电子邮件扫描**”。

   注释
   如果尚未配置 Outlook，则 Outlook 配置对话框启动。如果未登录到邮箱，系统会提示您登录。

这部分包含下列主题：

- 检测属性
- 高级属性
- 操作属性
- 警报属性
- 报告属性

检测属性

使用 “**检测**” 选项卡上的选项指定要扫描的附件和文件类型扩展名。

1 选择 “**检测**” 选项卡。

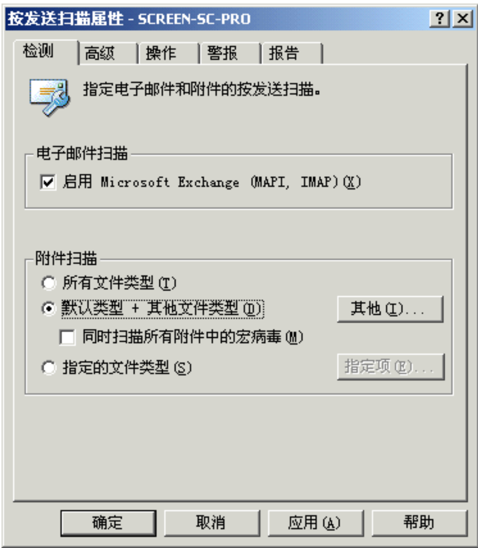


图 5-2. 按发送扫描属性 - 检测选项卡

2 在“**电子邮件扫描**”区域中，“**启用 Microsoft Exchange（MAPI、IMAP）**”是默认选择。如果不需要运行电子邮件扫描，请取消选择该选项。

3 在 “**附件扫描**” 区域中，选择下列选项之一：

- **所有文件类型**。该选项为默认选项。扫描所有附件，而无论其扩展名如何。

- **默认类型 + 其他文件类型**。扫描默认的扩展名列表以及您指定的任何其他内容。当前的 DAT 文件定义了默认的文件类型扩展名列表。您不能删除默认列表中的任何文件类型扩展名，但可以添加或删除用户指定的文件类型扩展名。

  - **其他**。如果选择了 “**默认类型 + 其他文件类型**”，请单击 “**其他**” 添加或删除用户指定的文件类型扩展名。详细说明，请参阅第 49 页的 “添加文件类型扩展名”。

    按发送电子邮件扫描程序列出的附加扩展名的最大数量为 1000。

  - **同时扫描所有附件中的宏病毒**。扫描所有附件的同时检查宏病毒，而无论扩展名为何。该选项仅在选择了 “**默认类型 + 其他文件类型**” 选项后才能使用。

- **指定的文件类型**。仅扫描您指定的扩展名。

  - **指定项**。如果选择了“**指定的文件类型**”，请单击“**指定项**”添加或删除用户指定的文件类型扩展名。还可以将文件类型扩展名列表设置为默认列表。详细说明，请参阅第 50 页的“添加用户指定的文件类型扩展名”。

    按发送电子邮件扫描程序列出的指定扩展名的最大数量为 1000。

注释
排除电子邮件扫描不支持的文件类型。

4 单击“**应用**”保存更改。

高级属性

使用“**高级**”选项卡的选项可以指定高级扫描属性，例如扫描未知程序病毒和可能有害的程序、压缩文件及电子邮件正文。

1 选择“**高级**”选项卡。

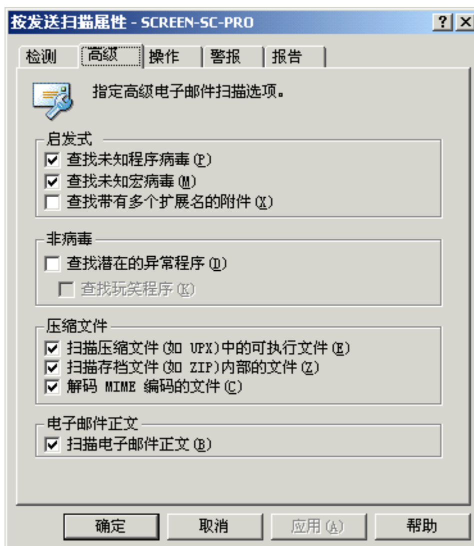


图 5-3. 按发送扫描属性 - 高级选项卡

2 在“**启发式**”区域中，指定是否要求扫描程序评估一段未知代码或 Microsoft Office 宏为病毒的概率。启用该功能后，扫描程序将分析它是已知病毒的变体的可能性。请选择以下选项的任意组合：

- **查找未知程序病毒**。该选项为默认选项。将含有类似病毒的代码的可执行文件作为真正感染了病毒的文件对待。扫描程序将应用您在 “**操作**” 选项卡中选择的操作。
- **查找未知宏病毒**。该选项为默认选项。将含有类似病毒的代码的嵌入式宏作为真正感染了病毒的文件对待。扫描程序将对这些文件应用您在 “**操作**” 选项卡中选择的操作。

注释
该选项不同于 “**检测**” 选项卡中的 “**同时扫描所有文件中的宏病毒**”，后面这个选项可指导扫描程序查找所有已知宏病毒。“**查找未知宏病毒**” 则指导扫描程序估计未知宏是病毒的概率。

- **查找带有多个扩展名的附件**。将带有多个扩展名的附件作为真正感染了病毒的附件对待。扫描程序将对这些文件应用您在 “**操作**” 选项卡中选择的操作。

  选择该选项时，屏幕上出现 “**电子邮件扫描警告**” 对话框。

  - **电子邮件扫描警告**。请仔细阅读警告。单击 “**确定**” 继续并接受对具有多个扩展名的感染病毒附件的处理选项，或者单击 “**取消**” 取消选择该选项。

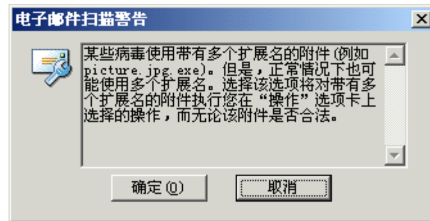


图 **5-4.** 电子邮件扫描警告

3 在 “**非病毒**” 区域中，指定是否要求扫描程序查找可能有害的非病毒程序。

- **查找潜在的异常程序**。查找潜在的异常程序，将其作为真正的染毒文件对待。
  - **查找玩笑程序**。如果选择了 “**查找潜在的异常程序**”，扫描程序还会扫描玩笑程序。

警告

VirusScan Enterprise 不清除可能有害的程序文件或玩笑程序。如果将扫描程序配置为 “**查找潜在的异常程序**” 和 / 或 “**查找玩笑程序**”，就不会清除检测到的任何程序或玩笑文件。

如果选定 “**清除感染病毒的附件**” 作为主要操作， VirusScan Enterprise 会自动执行辅助操作。如果选定 “**将感染病毒的附件移到文件夹**” 或 “**删除感染病毒的附件**”，则可能有合法的、已安装程序文件被移动或删除。移动或删除程序文件可能会留下注册表键、快捷方式和其他文件。

如果 VirusScan Enterprise 检测到您不想安装的可能有害的程序文件或玩笑程序，我们推荐您使用 Windows “**控制面板**” 中的 “**添加 / 删除程序**” 来完全卸载检测到的程序。您还可以联系 “**病毒信息库**”，了解有关手动卸载可能有害的程序的信息。

如果 VirusScan Enterprise 检测到您不想安装的可能有害的程序文件或玩笑程序，我们推荐您选择以下操作：

- 取消选择 “**查找潜在的异常程序**” 和 / 或 “**查找玩笑程序**” 选项。
- 排除检测到的程序文件名称。更多信息，请参阅第 51 页的 “排除文件、文件夹和驱动器”。

然后，重新安装该程序文件，如果该程序文件被移动，请从隔离文件夹中恢复，如果已删除，请从备份中恢复。

4 在 “**压缩文件**” 区域中，指定扫描程序要检查的压缩文件类型。您可以选择以下选项：

- **扫描压缩文件中的可执行文件**。该选项为默认选项。检查含有可执行文件的压缩文件。打包的可执行文件是运行时只将自己解压缩到内存中去的文件。打包的可执行文件永远不会解压缩到磁盘上。
- **扫描存档文件内部的文件**。该选项为默认选项。检查存档文件及其内容。存档文件是压缩文件，要访问它包含的文件，必须首先解压缩。存档所含文件在被写入磁盘时会经过扫描。
- **解码 MIME 编码的文件**。该选项为默认选项。检查 MIME 编码的文件。

注释

尽管该选项能够更好地保护用户，但扫描压缩文件还是增加了扫描所需的时间。

5 在 “**电子邮件正文**” 区域中，“**扫描电子邮件正文**” 是默认选择。如果不需要检查电子邮件消息的内容，请取消选择该选项。

6 单击 “**应用**” 保存更改。

操作属性

使用 “**操作**” 选项卡中的选项，指定希望扫描程序在发现病毒时所执行的主要和辅助操作。

1 选择 “**操作**” 选项卡。

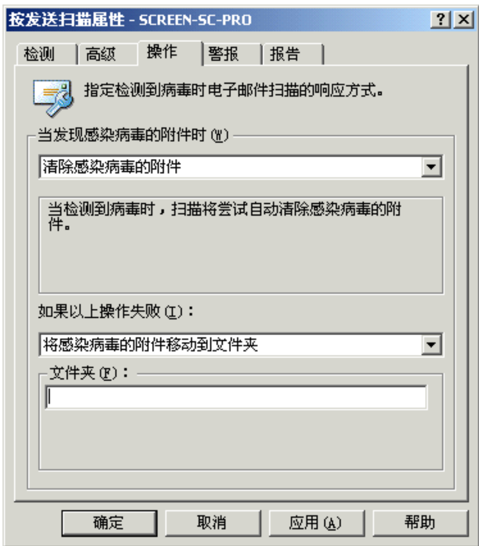


图 5-5. 按发送扫描属性 - 操作选项卡

2 在 “**当发现感染病毒的附件时**” 区域中，选择扫描程序将在发现病毒时采取的主要操作。

注释
默认的主要操作是 “**清除感染病毒的附件**”。

单击 ▼ 以选择如下操作之一：

- **操作提示**。提示用户在检测到病毒时采取何种操作。

  如果选择了这个选项，您还可以选择除停止和继续以外的操作。其他选择包括：

  - **清除附件**。允许清除附件感染的病毒。
  - **移动附件**。允许移动感染病毒的附件。
  - **删除附件**。允许删除感染病毒的附件。

  该选项不允许使用辅助操作。

- **继续扫描**。在发现感染病毒的附件后继续扫描。

  该选项不允许使用辅助操作。

- **将感染病毒的附件移动到文件夹**。将感染病毒的附件移到隔离文件夹。默认的隔离文件夹名称是 Quarantine。您可以接受隔离文件夹的默认名称，也可以输入新名称。

  注释
  quarantine 文件夹创建于 MAPI 数据库中，可从 Microsoft Outlook 中的 “**文件夹列表**”查看。

- **清除感染病毒的附件**。该选项为默认选项。扫描程序尝试删除感染病毒附件中的病毒。如果扫描程序无法删除附件中的病毒，或如果病毒已经把附件破坏到不可修复的程度，扫描程序将执行辅助操作。

- **删除感染病毒的附件**。一旦检测到病毒，扫描程序就会立即删除感染病毒的附件。请确保启用了 “**报告**”选项卡中的 “**记录到文件**”属性，以记录被感染了病毒的那些附件。

  如果选择此选项，您将被要求确认您的选择。单击 “**是**”确认所做选择，或单击 “**否**”取消此选项。

3 在 “**如果以上操作失败**”区域中，选择希望扫描程序在首选操作失败后采取何种辅助操作。

  注释
  默认的辅助操作是 “**将感染病毒的附件移动到文件夹**”。

  单击 ▾ 以选择如下操作之一：

  - **操作提示**。提示用户在检测到病毒时采取何种操作。

    如果选择了这个选项，您还可以选择除停止和继续以外的操作。其他选择包括：

    - **清除附件**。允许清除附件感染的病毒。如果已选择 “**清除感染病毒的附件**”为主要操作，则该选项被禁用。
    - **移动附件**。允许移动感染病毒的附件。如果已选择 “**移动感染病毒的附件**”为主要操作，则该选项被禁用。
    - **删除附件**。允许删除感染病毒的附件。如果已选择 “**删除感染病毒的附件**”为主要操作，则该选项被禁用。

  - **继续扫描**。在发现感染病毒的文件后继续扫描。

  - **将感染病毒的附件移到文件夹**。该选项为默认选项。将感染病毒的附件移到隔离文件夹。默认的隔离文件夹名称是 Quarantine。您可以接受隔离文件夹的默认名称，也可以输入新名称。

注释
Quarantine 文件夹创建于 MAPI 数据库中，可从 Microsoft Outlook 中的 “**文件夹列表**” 查看。

- **删除感染病毒的附件**。一旦检测到病毒，扫描程序就会立即删除感染病毒的附件。请确保启用了 “**报告**” 选项卡中的 “**记录到文件**” 属性，以记录被感染了病毒的那些附件。

  如果选择此选项，您将被要求确认您的选择。单击 “**是**” 确认所做选择，或单击 “**否**” 取消此选项。

4 单击 “**应用**” 保存更改。

警报属性

使用 “**警报**” 选项卡中的配置，可以配置检测到感染病毒的电子邮件或附件时发出警告的方式。

1 选择 “**警报**” 选项卡。

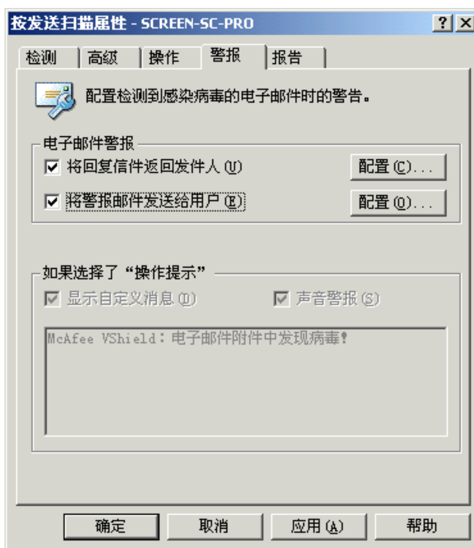


图 5-6. 按发送扫描属性 - 警报选项卡

2 在 “**电子邮件警报**” 区域中，指定检测到电子邮件病毒时如何通知发件人和其他用户。您可以选择以下选项：

- **将回复信件返回发件人**。向发件人发送回复邮件。
  - 如果选择了该选项，请单击 “**配置**” 打开 “**返回邮件配置**” 对话框。

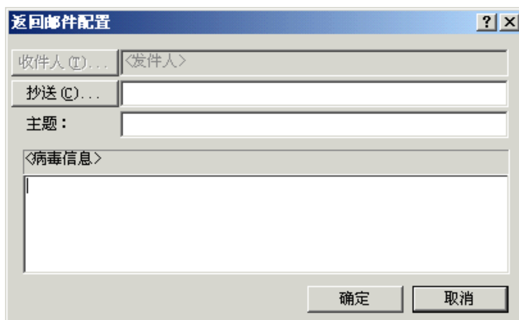


图 **5-7.** 电子邮件扫描 **-** 返回邮件配置

    - 输入要发送的内容，然后单击 “**确定**”。

- **将警报邮件发送给用户**。将电子邮件警报发送给其他用户。

    - 如果选择了该选项，请单击“**配置**”打开“**发送邮件配置**”对话框。

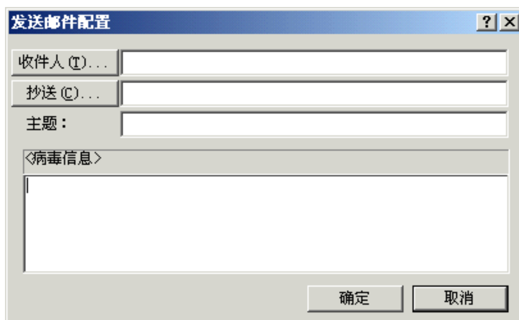


图 **5-8.** 电子邮件扫描 **-** 发送邮件配置

    - 输入要发送的内容，然后单击 “**确定**”。

3. 单击 “**应用**”保存更改。

4. 在 “**如果选择了 ‘操作提示’** ”区域中，指定检测到感染病毒的电子邮件时如何通知用户。您可以选择以下选项：

    - **显示自定义消息**。该选项为默认选项。用自定义消息通知用户。如果选择了该选项，您可以在文本框中输入自定义消息。

    - **声音警报**。该选项为默认选项。通过声音警报来通知用户。

5　单击 “**应用**”保存更改。

报告属性

使用“**报告**”选项卡上的选项配置日志活动。指定日志文件的位置和大小以及每个日志项要捕捉的信息。

1　选择 “**报告**”选项卡。



图 5-9. 按发送扫描属性 - 报告选项卡

活动日志文件可以作为一种重要的管理工具使用，它能够跟踪电子邮件中的病毒活动、记录用来检测和响应扫描程序发现的所有病毒的设置。以后复查时，可以从文本编辑器打开日志文件。此外，日志文件中记录的事件报告也有助于确定需要使用备份副本替换哪些文件、在隔离文件夹中检查哪些文件或者应从计算机中删除哪些文件。

2　在 “**日志文件**”区域中，从下列选项中进行选择：

- **记录到文件**。该选项为默认选项。在日志文件中记录按发送电子邮件扫描病毒活动。
- 接受文本框中默认的日志文件名称和位置，或者输入其他日志文件名称和位置，或者单击 “**浏览**”查找计算机或网络中的适当文件。

注释

默认情况下，扫描程序将日志信息写入如下目录中的 EMAILONDELIVERYLOG.TXT 文件中。

< 驱动器 >:Winnt\Profiles\All Users\Application Data\Network Associates\Virusscan

- **将日志文件大小限制为**。该选项为默认选项。默认日志文件大小是 1MB。接受默认的日志大小或设置不同的日志大小。如果选择了该选项，请输入一个介于 1MB 到 999MB 之间的值。

  注释

  如果日志文件中的数据超过了您设置的文件大小，则最早的百分之二十的日志条目将被删除，接着新数据会被添加到这个文件中。

3 在 “**记录内容**”区域中，选择要记录在日志文件中的其他信息：

- **会话设置**。记录您为日志文件中每个扫描会话所选择的属性。该选项不是默认选择。
- **会话摘要**。该选项为默认选项。摘要记录扫描程序在每个扫描会话过程中执行的扫描操作，并将该信息添加到日志文件。摘要信息包括已扫描的文件数、检测到的病毒数和类型、移动、清除或删除的文件数以及其他信息。该选项为默认选择。
- **日期和时间**。该选项为默认选项。记录检测到病毒时的日期和时间。该选项为默认选择。
- **用户名**。该选项为默认选项。这样即可将记录每个日志条目时登录到电子邮件的用户的姓名记录在日志文件中。该选项为默认选择。
- **扫描加密文件失败**。该选项为默认选项。在日志文件中记录那些扫描程序无法扫描的加密文件名称。该选项为默认选择。

4 单击 “**应用**”保存更改。

查看按发送电子邮件扫描结果

您可以在统计信息摘要和活动日志中查看扫描操作的结果。

这部分包含下列主题：

- 查看按发送电子邮件扫描统计信息
- 查看按发送电子邮件活动日志

查看按发送电子邮件扫描统计信息

“**按发送电子邮件扫描统计信息**”摘要显示了扫描程序已检查的文件数、找到的病毒数和以及采取的响应措施。

1. 打开 “**VirusScan 控制台**”。有关说明，请参阅第 18 页的 “VirusScan 控制台”。
2. 应用以下方法之一，打开 “**按发送电子邮件扫描统计信息**”对话框：
   - 突出显示任务列表中的任务，然后从“**任务**”菜单中选择“**统计信息**”。
   - 右键单击任务列表中的任务，然后选择 “**统计信息**”。

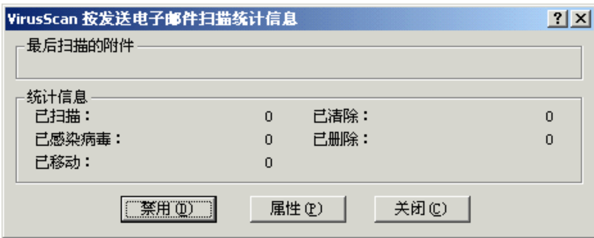


图 5-10. 按发送电子邮件扫描统计信息

   “**按发送扫描统计信息**”对话框的顶部窗格中显示了 “**最后扫描的附件**”，底部窗格中显示了统计信息摘要。

   如果扫描操作仍在运行，则显示扫描程序正在检查的文件以及扫描操作的状态。

3. 您可以使用如下功能之一：
   - 单击“**禁用**”以停止按发送扫描程序。这项功能可根据所选的操作切换。选择 “**禁用**”后，这一项又会变为 “**启用**”状态。要重新激活扫描程序，请单击同一对话框中的 “**启用**”。
   - 单击 “**属性**”打开 “**按发送电子邮件扫描属性**”对话框，然后根据需要更改扫描属性，并单击 “**应用**”保存更改。

     扫描将会立即采用新设置运行。

4 审阅过扫描统计信息之后，单击 “**关闭**”。

查看按发送电子邮件活动日志

按发送扫描活动日志显示了关于扫描操作的具体详细信息。例如，它可以显示扫描程序已检查的文件数、找到的病毒数以及采取的响应措施。

1 打开 “**VirusScan 控制台**”。有关说明，请参阅第 18 页的 “VirusScan 控制台”。

2 使用以下方法之一，打开活动日志文件：

- 突出显示任务，然后选择 “**任务**” 菜单中的 “**活动日志**”。
- 右键单击任务列表中的任务，并选择 “**查看日志**”。

3 要关闭活动日志，请选择 “**文件**” 菜单中的 “**退出**”。

按需电子邮件扫描

按需电子邮件扫描任务将根据需要从 Microsoft Outlook 直接运行，扫描所选电子邮件及其附件。使用按需电子邮件扫描程序，在已关闭 Microsoft Outlook 的情况下作为按发送电子邮件扫描程序的补充。

注释
如果在 VirusScan Enterprise 安装过程中打开了 Microsoft Outlook，我们建议在安装进程结束后重新启动 Microsoft Outlook。

这部分包含下列主题：

- 配置按需电子邮件任务
- 运行按需电子邮件任务
- 查看按需电子邮件扫描结果

配置按需电子邮件任务

您可以用 Microsoft Outlook 来配置按需电子邮件扫描任务，以便对邮件及附件进行扫描。要配置新的按需电子邮件扫描任务，请按照以下步骤操作：

1 启动 Microsoft Outlook。

2 采用以下方法之一，打开 “**按需电子邮件扫描属性**” 对话框：

- 选择 “**工具**” 菜单中的 “**电子邮件扫描属性**”。
- 单击 Outlook 工具栏中的 。

注释
如果该图标在 Outlook 工具栏中不可见，请单击标准工具栏右侧的 ，然后选择该图标。

这部分包含下列主题：

- 检测属性
- 高级属性
- 操作属性
- 警报属性
- 报告属性

检测属性

使用 “**检测**” 选项卡上的选项指定要扫描的附件和文件类型扩展名。

1 选择 “**检测**” 选项卡。

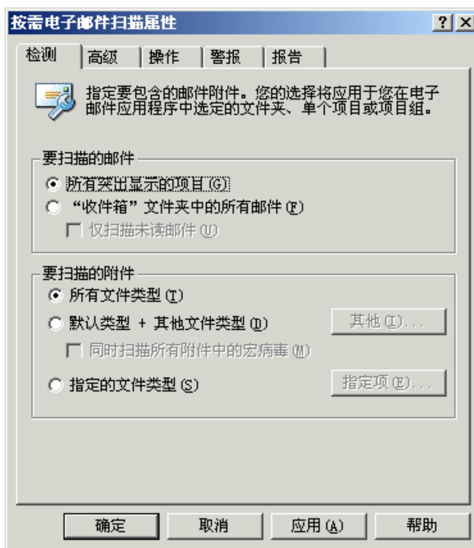


图 5-11. 按需电子邮件扫描属性 - 检测选项卡

2 在 “**要扫描的邮件**” 区域中，指定要扫描的邮件。您可以选择以下选项：

- **所有突出显示的项目**。该选项为默认选项。扫描选定的电子邮件或文件夹。

- **“收件箱”文件夹中的所有邮件**。扫描目前 **“收件箱”**文件夹及其子文件夹中的所有文件。
    - **仅扫描未读邮件**。扫描目前 **“收件箱”**文件夹及其子文件夹中的未读文件。如果未选择 **“‘收件箱’文件夹中的所有邮件”**，该选项将禁用。

3 在 **“要扫描的附件”**区域中，指定要扫描的文件、文件夹或驱动器。您可以选择以下选项：

- **所有文件类型**。该选项为默认选项。扫描所有附件，而无论其扩展名如何。
- **默认类型 + 其他文件类型**。扫描默认的扩展名列表以及您指定的任何其他内容。当前的 DAT 文件定义了默认的文件类型扩展名列表。您不能删除默认列表中的任何文件类型扩展名，但可以添加或删除用户指定的文件类型扩展名。
    - **其他**。如果选择了 **“默认类型 + 其他文件类型”**，请单击 **“其他”**添加或删除用户指定的文件类型扩展名。详细说明，请参阅第 49 页的 “添加文件类型扩展名”。

      按需电子邮件扫描程序列出的附加扩展名的最大数量为 1000。
    - **同时扫描所有附件中的宏病毒**。扫描所有附件的同时检查宏病毒，而无论扩展名为何。该选项仅在选择了 **“默认类型 + 其他文件类型”**选项后才能使用。
- **指定的文件类型**。仅扫描您指定的扩展名。
    - **指定项**。如果选择了 **“指定的文件类型”**，请单击 **“指定项”**添加或删除用户指定的文件类型扩展名。还可以将文件类型扩展名列表设置为默认列表。详细说明，请参阅第 50 页的 “添加用户指定的文件类型扩展名”。

      按需电子邮件扫描程序列出的指定扩展名的最大数量为 1000。

注释
排除电子邮件扫描不支持的文件类型。

4 单击 **“应用”**保存更改。

高级属性

使用“**高级**”选项卡的选项可以指定高级扫描属性，例如扫描未知程序病毒和可能有害的程序、压缩文件及电子邮件正文。

1 选择“**高级**”选项卡。

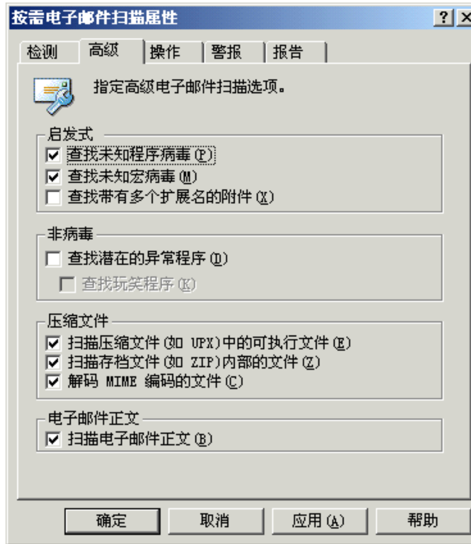


图 5-12. 按需电子邮件扫描属性 - 高级选项卡

2 在“**启发式**”区域中，指定是否要求扫描程序评估一段未知代码或 Microsoft Office 宏为病毒的概率。启用该功能后，扫描程序将分析它是已知病毒的变体的可能性。您可以选择以下选项：

- **查找未知程序病毒**。该选项为默认选项。将含有类似病毒的代码的可执行文件作为真正感染了病毒的文件对待。扫描程序将对这些文件应用您在“**操作**”选项卡中选择的操作。

- **查找未知宏病毒**。该选项为默认选项。将含有类似病毒的代码的嵌入式宏作为真正感染了病毒的文件对待。扫描程序将对这些文件应用您在“**操作**”选项卡中选择的操作。

  注释

  该选项不同于“**检测**”选项卡中的“**同时扫描所有文件中的宏病毒**”。该选项将指示扫描程序查找所有已知宏病毒。“**查找未知宏病毒**”则指导扫描程序估计未知宏是病毒的概率。

- **查找带有多个扩展名的附件**。将带有多个扩展名的附件作为真正感染了病毒的附件对待。扫描程序将对这些文件应用您在“**操作**”选项卡中选择的操作。

选择该选项时，屏幕上出现“**电子邮件扫描警告**”对话框。

- **电子邮件扫描警告**。请仔细阅读警告。单击“**确定**”继续并接受对具有多个扩展名的感染病毒附件的处理选项，或者单击“**取消**”取消选择该选项。

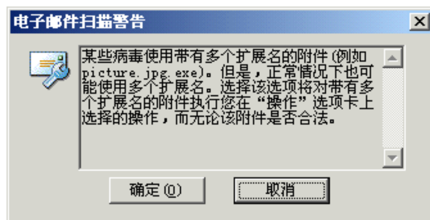


图 5-13. 电子邮件扫描警告

3 在“**非病毒**”区域中，指定是否要求扫描程序查找可能有害的非病毒程序。

- **查找潜在的异常程序**。查找潜在的异常程序，将其作为真正的染毒文件对待。
  - **查找玩笑程序**。如果选择了“**查找潜在的异常程序**”，扫描程序还会扫描玩笑程序。

警告

VirusScan Enterprise 不清除可能有害的程序文件或玩笑程序。如果将扫描程序配置为 “**查找潜在的异常程序**” 和 / 或 “**查找玩笑程序**”，就不会清除检测到的任何程序或玩笑文件。

如果选定 “**清除感染病毒的附件**”作为主要操作， VirusScan Enterprise 会自动执行辅助操作。如果选定 “**将感染病毒的附件移到文件夹**” 或 “**删除感染病毒的附件**”，则可能有合法的、已安装程序文件被移动或删除。移动或删除程序文件可能会留下注册表键、快捷方式和其他文件。

如果 VirusScan Enterprise 检测到您不想安装的可能有害的程序文件或玩笑程序，我们推荐您使用 Windows “**控制面板**”中的 “**添加 / 删除程序**”来完全卸载检测到的程序。您还可以联系 “**病毒信息库**”，了解有关手动卸载可能有害的程序的信息。

如果 VirusScan Enterprise 检测到您不想安装的可能有害的程序文件或玩笑程序，我们推荐您选择以下操作：

- 取消选择 “**查找潜在的异常程序**” 和 / 或 “**查找玩笑程序**”选项。
- 排除检测到的程序文件名称。更多信息，请参阅第 51 页的“排除文件、文件夹和驱动器”。

然后，重新安装该程序文件，如果该程序文件被移动，请从隔离文件夹中恢复，如果已删除，请从备份中恢复。

4 在 “**压缩文件**”区域中，指定扫描程序要检查的压缩文件类型。您可以选择以下选项：

- **扫描压缩文件中的可执行文件**。该选项为默认选项。检查含有可执行文件的压缩文件。打包的可执行文件是运行时只将自己解压缩到内存中去的文件。打包的可执行文件永远不会解压缩到磁盘上。
- **扫描存档文件内部的文件**。该选项为默认选项。检查存档文件及其内容。存档文件是压缩文件，要访问它包含的文件，必须首先解压缩。存档所含文件在被写入磁盘时会经过扫描。
- **解码 MIME 编码的文件**。该选项为默认选项。检查 MIME 编码的文件。

注释

尽管该选项能够更好地保护用户，但扫描压缩文件还是增加了扫描所需的时间。

5 在“**电子邮件正文**”区域中，“**扫描电子邮件正文**”是默认选择。如果不需要检查电子邮件消息的内容，请取消选择该选项。

6 单击 “**应用**”保存更改。

操作属性

使用“**操作**”选项卡中的选项，指定希望扫描程序在发现病毒时所执行的主要和辅助操作。

1 选择“**操作**”。

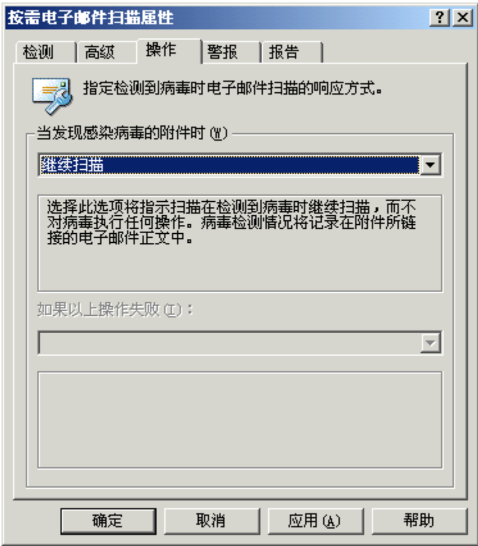


图 **5-14.** 按需电子邮件扫描属性 **-** 操作选项卡

2 在“**当发现感染病毒的附件时**”区域中，选择扫描程序将在发现病毒时采取的主要操作。

注释
默认的主要操作是“**清除感染病毒的附件**”。

单击 以选择如下操作之一：

- **操作提示**。提示用户在检测到病毒时采取何种操作。

如果选择了这个选项，您还可以选择除停止和继续以外的操作。其他选择包括：

- **清除附件**。允许清除附件感染的病毒。如果已选择 “**清除感染病毒的附件病毒**” 为主要操作，则该选项被禁用。
- **移动附件**。允许移动感染病毒的附件。如果已选择 “**移动感染病毒的附件**” 为主要操作，则该选项被禁用。
- **删除附件**。允许删除感染病毒的附件。如果已选择 “**删除感染病毒的附件**” 为主要操作，则该选项被禁用。

该选项不允许使用辅助操作。

- **继续扫描**。在发现感染病毒的附件后继续扫描。

  该选项不允许使用辅助操作。

- **将感染病毒的附件移到文件夹**。将感染病毒的附件移到隔离文件夹。默认的隔离文件夹名称是 Infected。您可以接受隔离文件夹的默认名称，也可以输入新名称。

  注释
  Infected 文件夹创建于 MAPI 数据库中，可从 Microsoft Outlook 中的 “**文件夹列表**” 查看。

- **清除感染病毒的附件**。该选项为默认选项。扫描程序尝试删除感染病毒附件中的病毒。如果扫描程序无法删除附件中的病毒，或如果病毒已经把附件破坏到不可修复的程度，扫描程序将执行辅助操作。
- **删除感染病毒的附件**。一旦检测到病毒，扫描程序就会立即删除感染病毒的附件。请确保启用了 “**报告**” 选项卡中的 “**记录到文件**” 属性，以记录被感染了病毒的那些附件。

  如果选择此选项，您将被要求确认您的选择。单击 “**是**” 确认所做选择，或单击 “**否**” 取消此选项。

3 在 “**如果以上操作失败**” 区域中，选择希望扫描程序在首选操作失败后采取何种辅助操作。

  注释
  默认的辅助操作是 “**将感染病毒的附件移到文件夹中**”。

  单击 ▾ 以选择如下操作之一：

  - **操作提示**。提示用户在检测到病毒时采取何种操作。

如果选择了这个选项，您还可以选择除停止和继续以外的操作。其他选择包括：

    - **清除附件**。允许清除附件感染的病毒。
    - **移动附件**。允许移动感染病毒的附件。
    - **删除附件**。允许删除感染病毒的附件。

- **继续扫描**。在发现感染病毒的文件后继续扫描。
- **将感染病毒的附件移到文件夹**。该选项为默认选项。将感染病毒的附件移到隔离文件夹。默认的隔离文件夹名称是 Infected。您可以接受隔离文件夹的默认名称，也可以输入新名称。

  注释

  Infected 文件夹创建于 MAPI 数据库中，可从 Microsoft Outlook 中的 “**文件夹列表**”查看。

- **删除感染病毒的附件**。一旦检测到病毒，扫描程序就会立即删除感染病毒的附件。请确保启用了 “**报告**”选项卡中的 “**记录到文件**”属性，以记录被感染了病毒的那些附件。

  如果选择此选项，您将被要求确认您的选择。单击 “**是**”确认所做选择，或单击 “**否**”取消此选项。

4 单击 “**应用**”保存更改。

警报属性

使用“**警报**”选项卡中的配置，以配置检测到感染病毒的电子邮件消息或附件时发出警告的方式。

1 选择 “**警报**”选项卡。

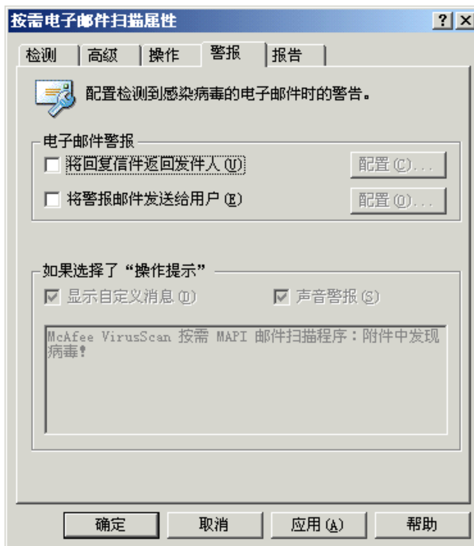


图 5-15. 按需电子邮件扫描属性 - 警报选项卡

2 在 “**电子邮件警报**”区域中，指定检测到电子邮件病毒时如何通知发件人和其他用户。您可以选择以下选项：

- **将回复信件返回发件人**。向发件人发送回复邮件。
  - 如果选择了该选项，请单击“**配置**”打开“**返回邮件配置**”对话框。

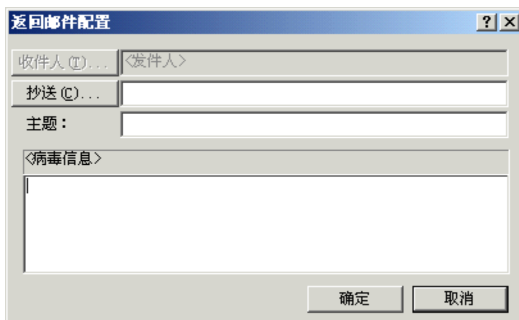


图 **5-16.** 电子邮件扫描 - 返回邮件配置

- 输入要发送的内容，然后单击 “**确定**”。

- **将警报邮件发送给用户**。将电子邮件警报发送给其他用户。
  - 如果选择了该选项，请单击“**配置**”打开“**发送邮件配置**”对话框。

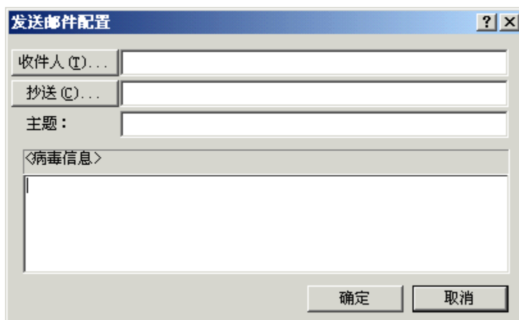


图 **5-17.** 电子邮件扫描 - 发送邮件配置

- 输入要发送的内容，然后单击 “**确定**”。

3 在 “**如果选择了 ‘操作提示’** ” 区域中，指定检测到感染病毒的电子邮件时如何通知用户。您可以选择以下选项：

- **显示自定义消息**。用自定义消息通知用户。如果选择了该选项，您可以在文本框中输入自定义消息。
- **声音警报**。通过声音警报来通知用户。

4 单击 “**应用**” 保存更改。

报告属性

使用“**报告**”选项卡上的选项配置记录活动。指定日志文件的位置和大小以及每个日志项要捕捉的信息。

1 选择“**报告**”选项卡。

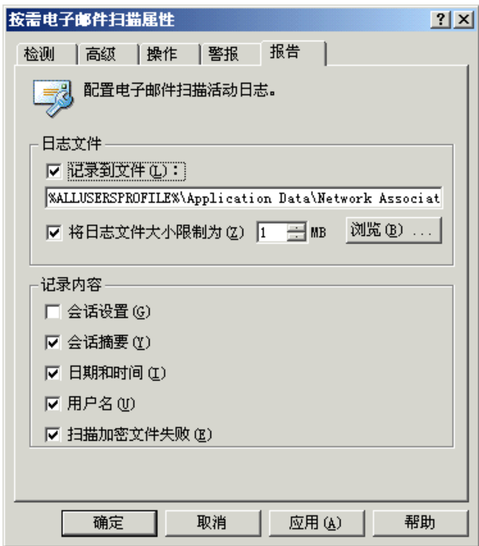


图 5-18. 按需电子邮件扫描属性 - 报告选项卡

日志文件可以作为一种重要的管理工具使用，它能够跟踪电子邮件中的病毒活动、记录用来检测和响应扫描程序发现的所有病毒的设置。以后复查时，可以从文本编辑器打开日志文件。此外，日志文件中记录的事件报告也有助于确定需要使用备份副本替换哪些文件、在隔离文件夹中检查哪些文件或者应从计算机中删除哪些文件。

2 在“**日志文件**”区域中，从下列选项中进行选择：

- **记录到文件**。该选项为默认选项。在日志文件中记录按需电子邮件扫描病毒活动。
- 接受文本框中默认的日志文件名称和位置，或者输入其他日志文件名称和位置，或者单击“**浏览**”查找计算机或网络中的适当文件。

注释

默认情况下，扫描程序将日志信息写入如下目录中的 EMAILONDEMANDLOG.TXT 文件中。

< 驱动器 >:Winnit\Profiles\All Users\Application Data\Network Associates\Virusscan

- **将日志文件大小限制为**。该选项为默认选项。默认日志文件大小是 1MB。接受默认的日志大小或设置不同的日志大小。如果选择了该选项，请输入一个介于 1MB 到 999MB 之间的值。

  注释
  如果日志文件中的数据超过了您设置的文件大小，则最早的百分之二十的日志条目将被删除，接着新数据会被添加到这个文件中。

3. 在 “**病毒活动以外的记录内容**” 区域中，选择要记录在日志文件中的其他信息：
   - **会话设置**。记录您为日志文件中每个扫描会话所选择的属性。该选项不是默认选择。
   - **会话摘要**。该选项为默认选项。摘要记录扫描程序在每个扫描会话过程中执行的扫描操作，并将该信息添加到日志文件。摘要信息包括已扫描的文件数、检测到的病毒数和类型、移动、清除或删除的文件数以及其他信息。该选项不是默认选择。
   - **日期和时间**。该选项为默认选项。记录检测到病毒时的日期和时间。该选项为默认选择。
   - **用户名**。该选项为默认选项。这样即可将记录每个日志条目时登录到计算机的用户的姓名记录在日志文件中。该选项为默认选择。
   - **扫描加密文件失败**。该选项为默认选项。在日志文件中记录那些扫描程序无法扫描的加密文件名称。该选项为默认选择。
4. 单击 “**应用**” 保存更改。

运行按需电子邮件任务

运行按需电子邮件扫描任务：

1. 启动 Microsoft Outlook。
2. 使用以下方法之一，从 Microsoft Outlook 启动按需电子邮件扫描：
   - 从 “**工具**” 菜单中，选择 “**扫描病毒**”。
   - 单击 Outlook 工具栏中的 。

   注释
   如果该图标在 Outlook 工具栏中不可见，请单击标准工具栏右侧的 ，然后选择该图标。



图 5-19. 按需电子邮件扫描

3 当按需电子邮件扫描结束后，关闭该对话框。

查看按需电子邮件扫描结果

扫描正在运行时，您可以在“**按需电子邮件扫描**”对话框中查看扫描结果，扫描结束后则可从活动日志查看结果。

这部分包含下列主题：

- 查看按需电子邮件活动日志

查看按需电子邮件活动日志

按需电子邮件扫描活动日志显示了关于扫描操作的详细信息。例如，它可以显示扫描程序已检查的附件数、找到的病毒数以及采取的响应措施。

1 查找到位于以下位置的 EMAILONDEMANDLOG.TXT 文件：

< 驱动器 >:Winnit\Profiles\All Users\Application Data\Network Associates\Virusscan

2 查看活动日志文件。

3 要关闭活动日志，请选择“**文件**”菜单中的“**退出**”。

病毒警报

6

VirusScan Enterprise 软件可采用多种方法通知您扫描活动的进程和结果。例如，当完成扫描操作之后，您可以在活动日志中查看任何扫描结果。此外，也可以在 VirusScan Enterprise 控制台上查看所有扫描的结果。但是，上述两种方法都不会在扫描程序检测到计算机上的病毒时立即通知您。尽管控制台能够实时显示扫描活动，但显然您不可能总是实时观看屏幕。警报管理器具有检测到病毒时立即通知您这一功能，该功能是集成到 VirusScan Enterprise 软件和其他 Network Associates 客户端 / 服务器安全和管理解决方案中的一个独立模块。

警报管理器可实时处理由防病毒软件生成的警报和事件。在典型配置中，警报管理器位于中央服务器上，监听网络客户机或服务器防病毒软件发送给它的警报。客户端软件可以是工作站或服务器应用程序。警报管理器允许您配置两种基本警报：

- 警报发送目的地和发送方式。
- 警报内容。

请参阅 《警报管理器产品指南》，获得更多信息。

这部分包含下列主题：

- 配置警报管理器
- 配置接收者与警报接收方式
- 自定义警报消息

配置警报管理器

使用“**警报属性**”对话框上的选项可以确定当扫描程序检测到病毒后何时以及如何通知您。

要打开 “**警报属性**”对话框，请执行以下步骤：

1 打开 “**VirusScan 控制台**”。有关说明，请参阅第 18 页的 “VirusScan 控制台”。

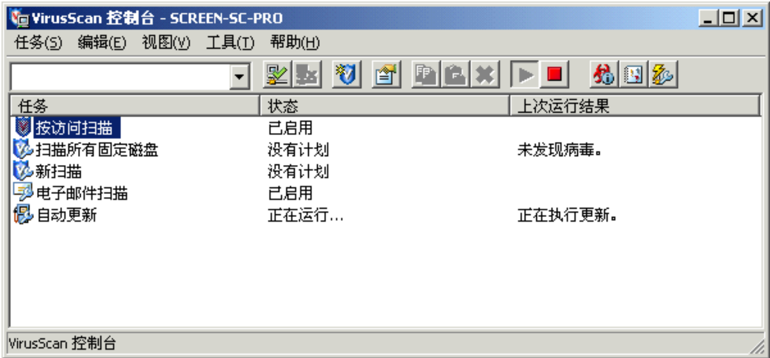


图 6-1. VirusScan 控制台

2 从 “**工具**”菜单中，选择 “**警报**”。

屏幕上将出现 “**警报属性**”对话框。

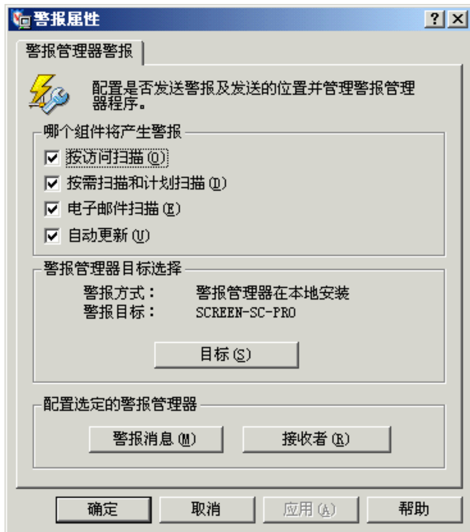


图 6-2. 警报属性

3 在 “**哪个组件将产生警报**”区域中，选择希望哪些组件与警报管理器通讯。选择以下选项的任意组合：

- **按访问扫描**。该选项为默认选择。
- **按需扫描和计划扫描**。该选项为默认选择。
- **电子邮件扫描**。该选项为默认选择。
- **自动更新**。该选项为默认选择。

4 在 “**警报管理器目标选择**”区域中，单击 “**目标**”打开 “**警报管理器客户端程序配置**”对话框。

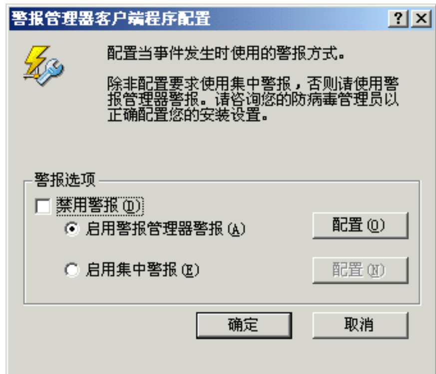


图 **6-3.** 警报管理器客户端程序配置

您可以禁用或启用警报功能，决定事件发生时所使用的警报方式，并指定接收警报的服务器。

a 在 “**警报选项**”区域中，指定满足需求的警报方式：.

- **禁用警报**。事件发生时不发送警报。
- **启用警报管理器警报**。该选项为默认选项。激活警报管理器警报方式。

  配置。如果选择了 “**启用警报管理器警报**”选项，单击 “**配置**”将打开 “**选择警报管理器服务器**”对话框。



图 **6-4.** 选择警报管理器服务器

在“**警报目的地**”区域中，输入“**接收警报的警报管理器服务器**”，或单击“**浏览**”查找位置。

单击“**确定**”保存更改并返回到“**警报管理器客户端程序配置**”对话框。

- **启用集中警报**。激活集中警报方式。集中警报是除常规警报管理器警报消息以外的另一种警报方法。更多信息，请参阅第 144 页的“使用集中警报”。

注释
考虑到共享文件夹的安全性问题， McAfee 建议您不使用集中警报。

配置。如果选择了“**启用集中警报**”选项，单击“**配置**”将打开“**集中警报配置**”对话框。

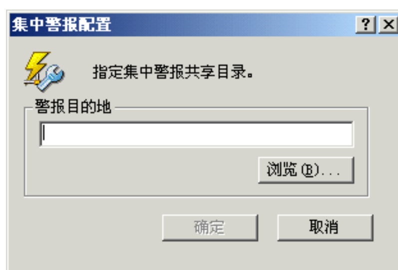


图 **6-5.** 集中警报配置

在“**警报目的地**”区域中，输入“**集中警报共享目录**”，或单击“**浏览**”查找位置。

单击“**确定**”保存更改并返回到“**警报管理器客户端程序配置**”对话框。

b 单击“**确定**”保存更改并返回到“**警报管理器**”对话框。

5 在“**配置选定的警报管理器**”区域中：

a 单击“**警报消息**”以配置“**警报管理器消息**”。详细说明，请参阅第 146 页的“自定义警报消息”。

注释
如果没有安装警报管理器，则“**警报消息**”按钮被禁用。

b 单击“**接收者**”以配置“**警报管理器属性**”。详细说明，请参阅第 122 页的“配置接收者与警报接收方式”。

注释
如果没有安装警报管理器，则 “**接收者**” 按钮被禁用。

c 单击 “**警报消息**” 以配置 “**警报管理器消息**”。详细说明，请参阅第 146 页的 “自定义警报消息”。

注释
如果没有安装警报管理器，则 “**警报消息**” 按钮被禁用。

d 完成配置 “**警报管理器属性**” 和 “**警报管理器消息**” 后，单击 “**确定**” 以关闭 “**警报属性**”。

配置接收者与警报接收方式

在 “**警报属性**” 对话框中，单击 “**接收者**” 打开 “**警报管理器属性**” 对话框。

“**警报管理器属性**” 对话框允许您配置警报管理器发出的警报消息的接收者以及接收者接收警报消息的方法。接收者可以是电子邮件地址，也可以是网络中的计算机。接收者既可以通过邮件消息、也可以通过网络弹出式消息来接收警报通知。

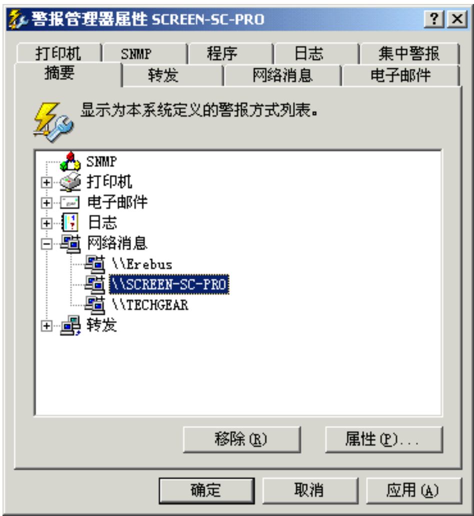


图 **6-6.** 警报管理器属性

要为特定警报方式配置接收者：

1 单击给定警报方式的相应选项卡，例如 “**日志**”。

2 配置使用这种方式接收警报通知的接收者。

3 单击其他选项卡，以便根据需要为其他任何警报方式配置接收者。

4 要在结束之后保存您的配置并关闭 “**警报管理器属性**”对话框，请单击 “**确定**”。

要详细了解如何配置特定的警报方式以及警报管理器通过这些方式向哪些接收者发送警报消息的信息，请参阅 “产品指南”的相关章节。

- 第 125 页的 “查看摘要页”。
- 第 126 页的 “将警报消息转发到其他计算机”。
- 第 129 页的 “以网络消息的形式发送警报”。
- 第 131 页的 “将警报消息发送到电子邮件地址”。
- 第 135 页的 “将警报消息发送到打印机”。
- 第 137 页的 “通过 SNMP 发送警报消息”。
- 第 138 页的 “将程序作为警报启动”。
- 第 140 页的 “在计算机的事件日志中记录警报通知”。
- 第 142 页的“向终端服务器发送网络消息”。仅当安装警报管理器的计算机上正在运行终端服务时，此方法才可用。
- 第 144 页的 “使用集中警报”。

关于添加警报方法的概述

您可以使用 “**警报管理器属性**”对话框中的多种选项卡来配置警报方法。将每种新方式添加到配置中时，都可以使用两个选项：

- 发送测试消息。
- 为接收者设置警报优先级。

发送测试消息

当使用“**警报管理器属性**”对话框中的选项卡添加新的警报通知接收者（例如网络计算机或电子邮件地址）时，您可以测试目标地址是否能够收到消息。要在配置某个方法时向选定的目标发送测试消息，请单击 “**测试**”按钮。

如果所有配置都正确，这条消息会出现在所配置的目标位置。

注释

邮件警报可能要花费一段时间到达目的地，这取决于您的 SMTP 服务器和接收方的电子邮件服务器。

测试消息没有到达目标

如果目标计算机收不到这条消息，请查看如下列表并根据实际情况确认：

- 已经启用实施所选警报方法所需的通讯服务，例如电子邮件或 SNMP。

- 发送或接收这条消息所必需的设备 （例如调制解调器或寻呼机）存在而且运行正常。
- 为响应病毒检测而需要运行的所有程序都位于指定的路径中，并且安装正确。
- 作为目标的任何打印机或计算机都存在于网络中。
- 网络正常运行。
- 您提供的配置信息正确而且完整。某些属性页包括二级页面。例如，“**电子邮件属性**”页可链接到 “**邮件设置**”页。确保查看了二级页面的信息。
- 如果安装警报管理器时使用了帐户和密码，请确保指定的帐户具有足够权限，可以执行您试图进行的操作。

为接收者设置警报优先级

可以为添加到警报管理器配置中的每个接收者指定优先级。警报管理器只向指定的接收者 （例如电子邮件地址）发送同级或优先级更高的警报通知。

这对于过滤警报通知而言非常有用。例如，使用 “**警报管理器属性**”对话框中的 “**日志**”选项卡，您可以在计算机的事件日志中记录各种优先级的警报消息 （请参阅第 140 页的 “在计算机的事件日志中记录警报通知”）。当然，您也可能希望警报管理器只通过电子邮件向网络管理员的寻呼机发送严重的警报通知。为此，请为记录和电子邮件接收者分别设置优先级阀值。

为具体接收者设置警报优先级：

1. 在某个警报方法的 “**属性**”对话框中单击 “**优先级**”按钮。

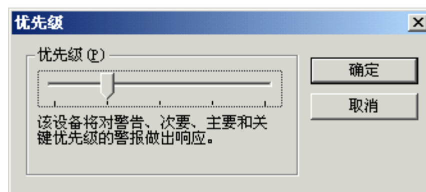


图 **6-7.** 优先级

2. 在 “**优先级**”对话框中，向右或向左拖动滑块以设置优先级。

   向右拖动，表示向接收者发送的警报消息数量较少，但优先级较高。将滑块拖动到左侧，则可以向接收者发送更多警报消息，包括优先级较低的那些消息。

3. 单击 “**确定**”保存优先级设置。

注释

在 “**优先级**”对话框中，您可以为特定的接收者 （例如网络中的计算机或电子邮件地址）指定优先级。但是，**不能**在此设置个别警报消息的优先级。要为个别警报设置优先级，请参阅第 146 页的 “自定义警报消息”。

查看摘要页

“**警报管理器属性**”对话框中的 “**摘要**”选项卡上列出了警报管理器将向其发送它所收到的警报通知的接收者。系统将按警报方法对接收者进行分组。

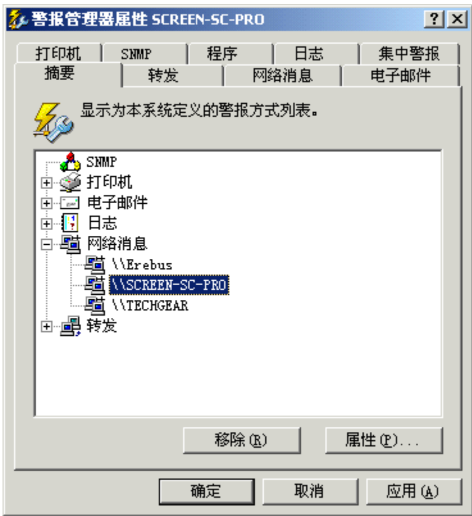


图 6-8. 警报管理器属性 - 摘要选项卡

单击所列出的每种警报方式旁边的⊞可以显示作为接收方的计算机、打印机或电子邮件地址。要移除警报通知接收者，请选择它，然后单击 “**移除**”。要为列出的接收者更改配置选项，请选择该接收者，然后单击 “**属性**”打开这种警报方法的 “**属性**”对话框。

安装警报管理器时，默认配置是向安装警报管理器的计算机发送弹出式网络消息，并将警报通知记录在这台计算机的事件日志中。因此，如果您还没有为警报管理器配置警报通知的接收者，则 “**摘要**”选项卡只显示这两种方式。警报管理器会为这两种默认方式设置优先级，以便发送除最低优先级 （“**信息**”）以外的所有优先级警报通知。关于优先级的详细信息，请参阅第 124 页的 “为接收者设置警报优先级”。

以下章节描述了每种方法的可用选项。

将警报消息转发到其他计算机

警报管理器可以将从 McAfee 防病毒客户端或服务器产品接收到的警报消息转发给网络中安装有警报管理器软件的其他计算机。通常情况下，如果需要将消息转发给另一台警报管理器服务器来扩大分发范围时，才需要执行此操作。

> **注释**
> 警报管理器 4.7 只能与运行同一版本的警报管理器的服务器相互转发警报通知。如果服务器运行较早版本的警报管理器，则它们之间不能相互转发警报通知。

在大型公司中转发警报

如果公司规模很大，则您可以使用转发功能将警报通知发送到中央通知系统或 MIS（管理信息系统）部，以便跟踪病毒统计资料和问题区域。此外，大型公司会超出地理界限，分支机构可能会分布在几个不同的国家。在这种情况下，您可能希望在本地服务器上安装一个警报管理器以处理来自本地子网络中的警报。您可以将本地警报管理器服务器配置为将优先级较高的警报通知转发给网络中其他位置的服务器，以便于将来分发。

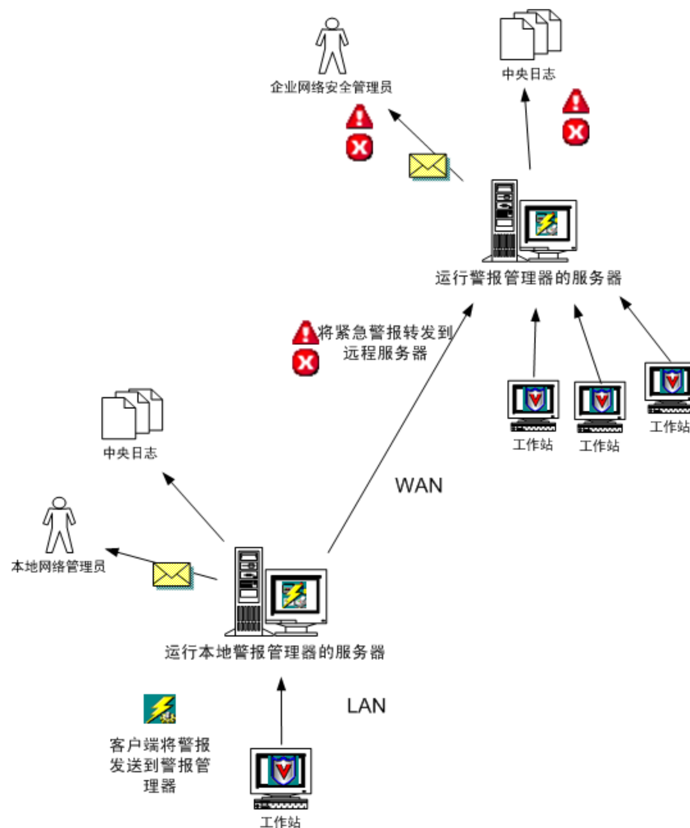


图 6-9. 将警报转发给另一个警报管理器

为此，请将本地的警报管理器配置为将相关警报转发到安装有第二个警报管理器的计算机。然后，您需要配置第二个警报管理器根据需要分发警报通知。有关该操作的详细信息，请参阅第 128 页的 “配置警报转发选项”。

在小型公司中转发警报

在规模较小的公司中，转发功能同样非常有用。假设您希望将优先级较高的所有警报通知通过电子邮件发送给特定的寻呼机，但是网络中只有一台服务器与 Internet 直接连接。

要解决这一问题：

1. 在每台警报管理器服务器上配置警报管理器，以便将优先级较高的警报消息转发到安装有调制解调器的计算机中。
2. 然后配置这些计算机上的警报管理器，以便将优先级较高的警报发送到目标寻呼机的电子邮件地址。

配置警报转发选项

配置转发选项：

1 单击 “**警报管理器属性**”对话框中的 “**转发**”选项卡。

“**转发**”页将显示您选择要接收转发消息的所有计算机列表。如果尚未选择目标计算机，则该列表为空。

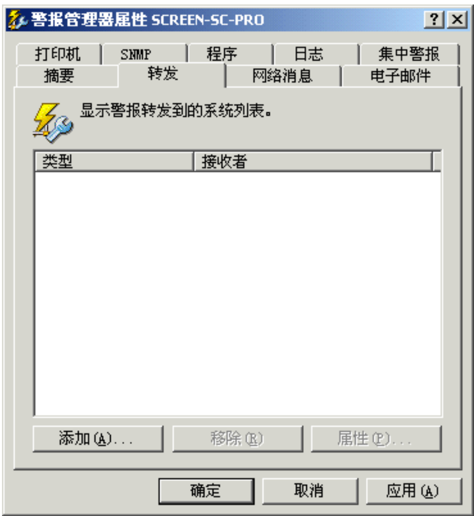


图 **6-10.** 警报管理器属性 **-** 转发选项卡

2 要更新该列表，请执行如下任一操作：

- 要添加计算机，请单击 “**添加**”打开 “**转发**”属性对话框，然后在文本框中输入要接收转发消息的计算机名称。可以按照通用命名标准 (UNC) 输入计算机的名称，或者单击 “**浏览**”在网络中查找计算机。
- 要删除列出的计算机，请选择一个列出的目标计算机，然后单击 “**移除**”。
- 要更改配置选项，请选择一个列出的目标计算机，然后单击 “**属性**” 。警报管理器将打开 “**转发**”属性对话框。输入要从警报管理器接收转发消息的计算机名称，或者单击 “**浏览**”在网络中查找计算机。



图 6-11. 转发属性

3 单击“**优先级**”指定目标计算机要接收哪种警报消息。请参阅第 124 页的“为接收者设置警报优先级”。

4 单击“**测试**”向目标计算机发送一条测试消息。请参阅第 123 页的“发送测试消息”。

5 单击 “**确定**”返回到 “**警报管理器属性**”对话框。

以网络消息的形式发送警报

警报管理器可将警报发送到其他计算机。目标计算机的屏幕上将显示标准的弹出式消息框，并要求接收者确认该消息。

接收者的计算机无需安装警报管理器。然而，您可能需要针对接收者的计算机操作系统安装适当的客户端通讯软件。这个通讯软件通常预装在较新版本的 Windows 操作系统 （例如 Windows NT、 Windows 2000 和 Windows XP）中。默认情况下，这项服务总是在运行中。

要配置警报管理器以便将警报通知作为网络消息发送，请执行如下步骤：

1 打开 “**警报管理器属性**”对话框。

2 单击“**网络消息**”选项卡。“**网络消息**”页中将显示已配置为接收网络消息的计算机列表。如果尚未选择接收计算机，则该列表为空。

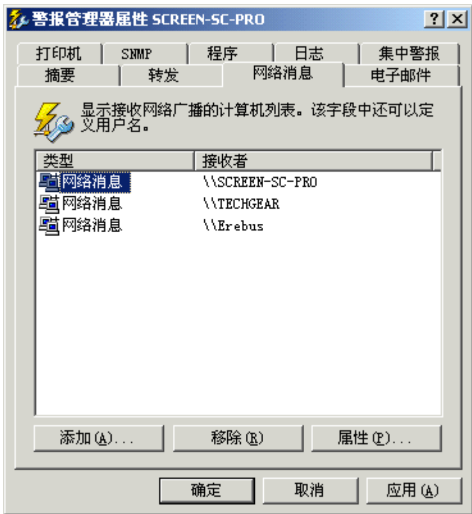


图 6-12. 警报管理器属性 - 网络消息选项卡

3 要更新该列表，请执行如下任一操作：

- 要添加计算机，请单击 "**添加**" 打开 "**网络消息**" 属性对话框。您可以通过两种方式指定接收计算机。以 UNC 格式直接在 "**计算机：**" 文本框中输入计算机的名称，或者选择 "**浏览**" 查找网络中的计算机。
- 要移除列出的计算机，请选择一个列出的接收者名称，然后单击 "**移除**"。
- 要更改配置选项，请选择一个列出的接收者名称，然后单击 "**属性**" 。警报管理器将打开 "**网络消息**" 属性对话框。根据需要更改 "**计算机：**" 文本框中的信息。

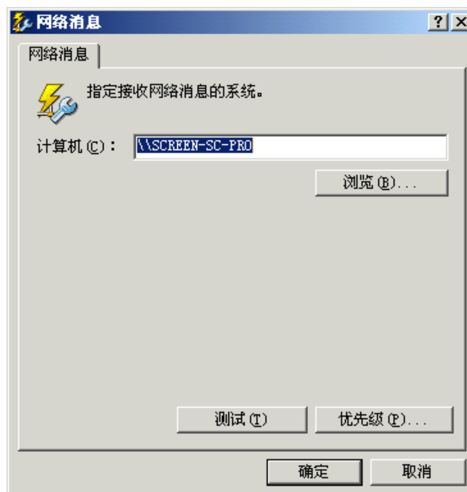


图 **6-13.** 网络消息属性

4 单击“**优先级**”指定接收者要接收的警报消息类型。请参阅第 124 页的“为接收者设置警报优先级”。

5 单击 “**测试**” 向接收者发送一条测试消息。请参阅第 123 页的 “发送测试消息”。

6 单击 “**确定**” 返回到 “**警报管理器属性**” 对话框。

将警报消息发送到电子邮件地址

警报管理器可通过简单邮件传输协议 (SMTP) 将警报发送到接收者的电子邮件地址。警报消息显示在接收者的邮箱中。如果消息非常紧急，您可以用其他方法作为电子邮件消息的补充 （例如弹出式网络消息），以确保接收者及时看到警报并采取适当措施。

注释

邮件警报可能要花费一段时间到达目的地，这取决于您的 SMTP 服务器和接收方的电子邮件服务器。

要将警报管理器配置为以电子邮件的形式发送警报通知，请执行如下步骤：

1 打开 “**警报管理器属性**” 对话框。

2 单击 “**电子邮件**” 选项卡。

“**电子邮件**”页将显示您选择接收警报消息的电子邮件地址列表。如果尚未选择电子邮件地址，则该列表为空。

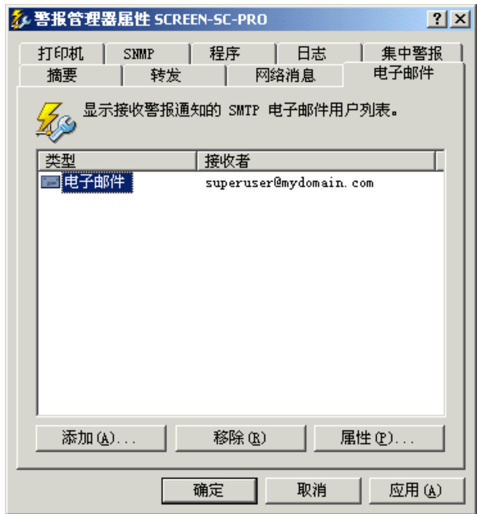


图 **6-14.** 警报管理器属性 **-** 电子邮件选项卡

3 要更新该列表，请执行如下任一操作：

- 要将一个电子邮件地址添加到列表中，请单击 “**添加**”打开 “**电子邮件**”属性对话框。在 “**地址**”文本框中输入警报通知接收者的电子邮件地址，在 “**主题**”文本框中输入主题，然后在 “**发件人**”文本框中输入您的电子邮件地址。使用标准的 Internet 地址格式 < 用户名 >@< 域 > （例如 administrator_1@mail.com）。

  控制对较长消息的截短（例如，包含特别长的文件名和路径名的消息，会在地址上附加一个 “*” 号），例如：`administrator_1@mail.com*`。详细信息，请参阅第 135 页的“强制截短发送给特定电子邮件地址的消息”。

- 要删除列出的地址，请选择一个电子邮件地址，然后单击 “**移除**”。

- 要更改配置选项，请选择一个列出的电子邮件地址，然后单击“**属性**”。警报管理器将打开 “**电子邮件**”属性对话框。如有必要，可更改文本框中的信息。



图 **6-15.** 电子邮件属性

4 单击 “**邮件设置**”指定用来通过 SMTP 发送 Internet 邮件的网络服务器。

注释

您必须单击 “**邮件设置**”并指定能够发送电子邮件警报通知的 SMTP 服务器。请勿跳过这一步。此外，第一次配置 SMTP 邮件设置后，只有当 SMTP 邮件服务器信息发生改变时，才需要再次配置它们。



图 6-16. SMTP 邮件设置

a 在出现的对话框中，输入邮件“**服务器**”。此服务器名称应以 Internet 协议 (IP) 地址、本地域名服务器能够识别的名称或者通用命名标准 (UNC) 符号的形式输入。

b 如果 SMTP 服务器要求，还需要键入在邮件服务器上使用的 “**登录**” 名称。

注释
如果您的 SMTP 邮件服务器被配置为使用登录名，请只在 “**登录**” 字段中输入登录名。请检查您的 SMTP 配置以确定是否需要这样做。若您的邮件服务器未配置为使用您输入的登录名，会导致电子邮件警报问题。

c 单击 “**确定**” 返回到 “**电子邮件**” 属性对话框。

5 单击“**优先级**”指定接收者的计算机要接收的警报消息类型。请参阅第 124 页的 “为接收者设置警报优先级”。

6 单击“**测试**”向接收者的计算机发送一条测试消息。请参阅第 123 页的“发送测试消息”。

7 如果测试消息发送成功，单击 “**确定**” 返回到 “**警报管理器属性**” 对话框。

强制截短发送给特定电子邮件地址的消息

有时警报通知消息会变的非常长，尤其当消息中的 `%FILENAME%` 系统变量含有非常长的文件路径和名称时。包含长文件名的复杂消息容易造成混乱，也不便于使用。例如，将电子邮件发送到寻呼机时，某些寻呼机服务会强制将长消息截短，这样就可能会删除消息中的重要信息。另一方面，如果非常长的消息实际传送到了寻呼机，接收者也必须滚动浏览文件名中的路径信息才能阅读警报中的关键信息。

有两个选项可以用于管理电子邮件警报通知中的长消息。

- 在电子邮件地址后附加一个星号 (*)，例如 `administrator_1@mail.com*`。警报管理器会根据当前系统的 SMTP 消息长度设置，截短发送到带有星号的电子邮件地址中的警报。默认的 SMTP 长度为 240 个字符。

  当警报管理器通过电子邮件向寻呼机发送警报时，这一设置非常有用。某些寻呼机服务的消息长度限制得非常短，例如 200 个字符。如果消息是通过电子邮件传送到寻呼机，则会在地址后附加一个星号 (*)，这样您而非寻呼服务公司就可以控制是否截短这条消息。

- 您也可以在 “**警报管理器消息**” 对话框中编辑消息文本，以确保重要的消息内容尽可能多的保留在被截短后的消息中。为此，您可以缩写信息的某些部分，也可以将重要信息移到消息的开头，这样可以将长文件名放在消息的后部。

将警报消息发送到打印机

警报管理器可以向打印机发送警报消息，以便打印出硬拷贝的消息。将警报管理器配置为将警报通知发送到打印队列：

1. 打开 “**警报管理器属性**” 对话框。
2. 单击 “**打印机**” 选项卡。

   “**打印机**” 页将显示您选择要接收警报消息的所有打印机队列列表。如果尚未选择打印机队列，则该列表为空。

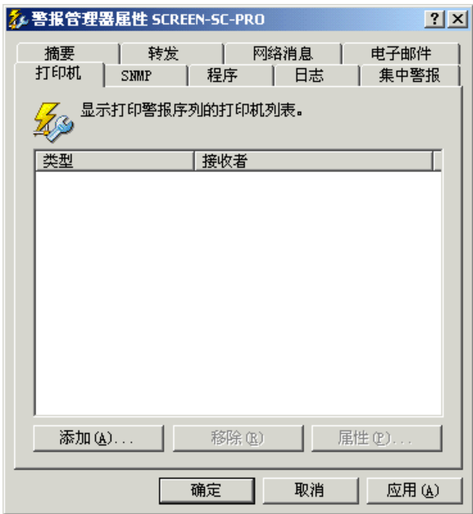


图 6-17. 警报管理器属性 - 打印机选项卡

3 要更新该列表，请执行如下任一操作：

- 要向列表添加打印队列，请单击 “**添加**”打开 “**打印机**”属性对话框，然后输入要将消息发送到其中的打印队列名称。您可以输入打印队列名称，或者单击 “**浏览**”，查找网络中的打印队列。
- 要移除列出的打印队列，请在列表中选择一项，然后单击 “**移除**”。
- 要更改配置选项，请选择一个列出的打印机，然后单击 “**属性**”。警报管理器将打开 “**打印机**”属性对话框。如有必要，更改 “**打印机**”文本框中的信息。



图 6-18. 打印机属性

4 单击 “**优先级**” 指定接收打印机要接收的警报通知类型。请参阅第 124 页的 “为接收者设置警报优先级”。

5 单击 “**测试**” 向接收打印机发送一条测试消息。请参阅第 123 页的 “发送测试消息”。

6 单击 “**确定**” 返回到 “**警报管理器属性**” 对话框。

通过 SNMP 发送警报消息

警报管理器可通过简单网络管理协议 (SNMP) 将警报消息发送到其他计算机。要使用该选项，您必须在计算机上安装并激活 Microsoft SNMP 服务。详细说明，请参阅操作系统文档。要查看客户端防病毒软件发送的警报消息，还必须使用 SNMP 查看器正确配置 SNMP 管理系统。要了解如何安装和配置 SNMP 管理系统，请参阅 SNMP 管理产品的文档。

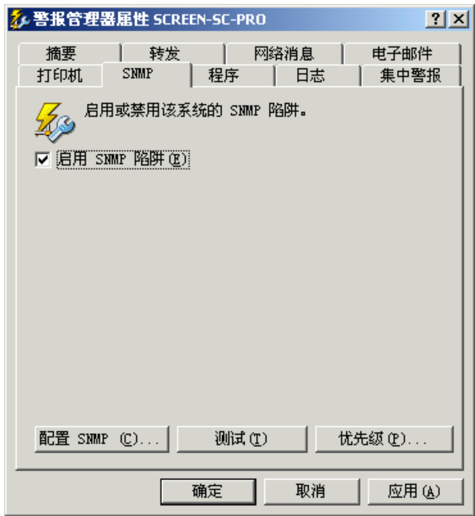


图 **6-19.** 启用 **SNMP** 警报

配置扫描程序以便通过 SNMP 发送警报消息：

1. 打开 “**警报管理器属性**” 对话框。
2. 单击 “**SNMP**” 选项卡。
3. 选择 “**启用 SNMP 陷阱**”。
4. 如果安装了警报管理器的计算机上运行的是 Windows NT 4 操作系统，请单击 “**配置 SNMP**” 以显示 Windows “**网络**” 对话框，并配置 Microsoft SNMP 服务。详细说明，请参阅操作系统文档。
5. 单击 “**优先级**” 指定接收者的计算机要接收的警报消息类型。请参阅第 124 页的 “为接收者设置警报优先级”。
6. 单击 “**测试**” 通过 SNMP 向接收计算机发送一条测试消息。请参阅第 123 页的 “发送测试消息”。
7. 单击 “**确定**” 保存更改并返回到 “**警报管理器属性**” 对话框。

将程序作为警报启动

每当收到表明发现病毒的警报时，警报管理器可以自动启动计算机或网络上的任意一个可执行程序。默认情况下，警报管理器会运行 VIRNOTFY.EXE，该程序安装在警报管理器的安装目录下。VIRNOTFY.EXE 会在安装警报管理器的计算机显示器上将感染病毒的文件名称显示在一个滚动对话框中。

注释

警报管理器仅在收到专门关于病毒的警报时才启动程序。警报消息中必须包含系统变量 %VIRUSNAME% 和 %FILENAME%。请参阅第 150 页的 "使用警报管理器系统变量"。警报管理器将不启动任何程序，除非警报中包含这些字段，而不管该程序所设置的优先级如何。关于优先级的更多信息，请参阅第 124 页的 "为接收者设置警报优先级"。

将警报管理器配置为在发现病毒时执行程序：

1 打开 "**警报管理器属性**" 对话框。

2 单击 "**程序**" 选项卡打开 "**程序**" 页。

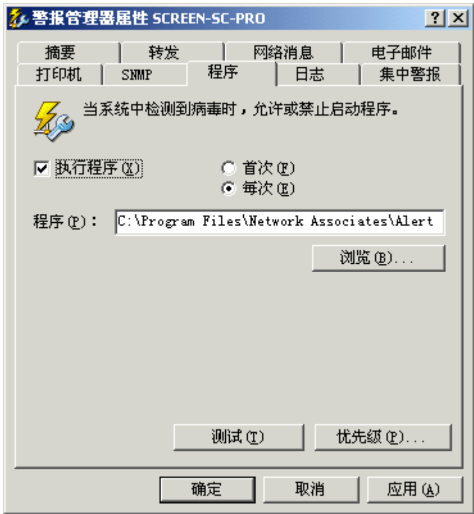


图 6-20. 警报管理器属性 - 程序选项卡

3 选择 "**执行程序**"。

4 输入当防病毒软件发现病毒时要运行的可执行程序的名称和路径，或者单击 "**浏览**" 在计算机或网络中找到这个程序文件。

5 选择以下操作之一：

- 如果需要仅在防病毒软件首次发现某个特定病毒时启用该程序，请单击 "**首次**" 按钮。
- 要在扫描程序每次发现病毒时都启动该程序，请单击 "**每次**"。

注释

如果选择了 “**首次**”，则当扫描程序第一次发现特定的病毒 （例如 VirusOne）时，您指定的程序就会启动。如果在同一个文件夹中多次发现 VirusOne，则扫描程序也不会再次启动该程序。但是，如果发现 VirusOne 后又查找到不同的病毒 (VirusTwo)，随后又检测到 VirusOne，则每次检测到病毒时都会启动该程序。在本示例中，会连续启动三次。多次启动同一个程序可能会导致服务器内存不足。

6 单击“**优先级**”指定接收者的计算机要接收的警报消息类型。请参阅第 124 页的 “为接收者设置警报优先级”。

   请注意，“**程序**”这种方法不会运行某个程序，除非警报是专门关于病毒的。也就是说，警报中必须包含系统变量 `%VIRUSNAME%` 和 `%FILENAME%`。所有其他警报都将被忽略，不论其优先级如何。

7 单击“**测试**”向接收者的计算机发送一条测试消息。请参阅第 123 页的“发送测试消息”。

在计算机的事件日志中记录警报通知

警报管理器可以将警报消息记录到本地计算机或网络中其他计算机的事件日志中。

配置记录选项：

1 打开 “**警报管理器属性**”对话框。

2 单击 “**日志**”选项卡。

   “**日志**”页显示了您选择要接收记录消息的所有计算机列表。如果尚未选择接收计算机，则该列表为空。

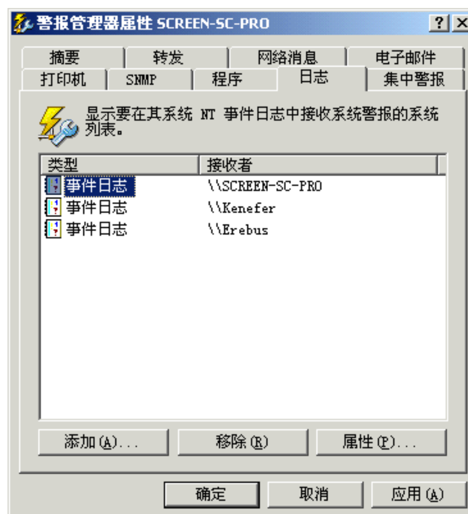


图 6-21. 警报管理器属性 - 日志选项卡

3 要更新该列表，请执行如下任一操作：

- 要添加计算机，请单击 “**添加**” 打开 “**日志**” 属性对话框，然后在文本框中输入接收转发消息的计算机名称。可按通用命名标准 (UNC) 输入计算机名称，也可以单击 “**浏览**” 在网络中查找计算机。
- 要删除列出的计算机，请单击列表中的一项，然后单击 “**移除**”。
- 要更改配置选项，请选择一个列出的接收计算机，然后单击 “**属性**” 。警报管理器将打开 “**日志**” 属性对话框。输入您希望警报管理器将消息转发到哪个计算机以进行记录。单击 “**浏览**” 查找目标计算机。



图 **6-22.** 记录属性

4 单击“**优先级**”指定接收者的计算机要接收的警报消息类型。请参阅第 124 页的 “为接收者设置警报优先级”。

5 单击“**测试**”向接收者的计算机发送一条测试消息。请参阅第 123 页的“发送测试消息”。

6 单击 “**确定**”返回到 “**警报管理器属性**”对话框。

向终端服务器发送网络消息

警报管理器可以向终端服务器发送警报消息。弹出式网络消息会向用户显示产生警报的会话。

如果运行警报管理器的计算机是终端服务器，则 “**警报管理器属性**”对话框只显示 “**终端服务器**”选项卡。

将警报管理器配置为将警报消息发送到终端服务器：

1 打开 “**警报管理器属性**”对话框。

2 单击 “**终端服务器**”选项卡。

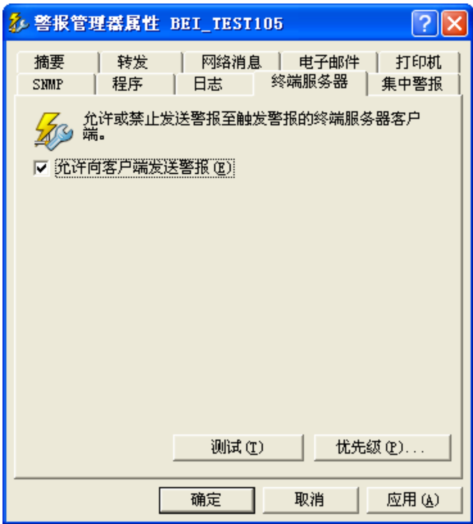


图 6-23. 警报管理器属性 - 终端服务器选项卡

3 要启用终端服务器警报，请选择 “**允许向客户端发送警报**”。

4 单击 “**测试**” 向接收者的计算机发送一条测试消息。屏幕上将显示 “**选择客户端以将‘终端服务器’测试消息发送至**”，其中列出了该计算机的当前终端服务器用户会话。



图 6-24. 向终端服务器用户发送一条测试消息

5 从列表中选择一个用户，然后单击 “**确定**” 向这名用户发送测试消息并返回到 “**警报管理器属性**” 对话框。

6 单击 “**优先级**” 指定终端服务器用户要接收的警报消息类型。请参阅第 124 页的 “为接收者设置警报优先级”。

7 单击 “**确定**” 保存终端服务器设置并返回到 “**警报管理器属性**” 对话框。

使用集中警报

集中警报是除常规警报管理器通知方法以外的另外一种消息发送方法。使用集中警报，可以将防病毒软件（例如 VirusScan Enterprise 7.0）生成的警报消息保存在服务器上的一个共享文件夹中。然后将警报管理器配置为从同一个文件夹读取警报通知。共享文件夹中的内容如果改变，警报管理器将按照配置好的方式发送新警报通知，如向寻呼机发送电子邮件消息。

警告
考虑到共享文件夹的安全性问题， McAfee 建议您不使用集中警报。相反，您应该将您的客户端防病毒软件配置为使用警报管理器的常规警报通知方法。

如果您决定选用集中警报，请按照以下步骤进行配置：

1 配置客户端计算机上的防病毒软件，以便将警报消息发送到相应的警报文件夹中。请参阅防病毒软件文档来了解如何配置集中警报。

注释
要允许网络中的其他工作站将消息发送到这个文件夹，必须为所有用户和计算机提供对该文件夹的文件扫描、写、创建和修改权限。详细说明，请参阅操作系统文档。

2 请确保所有用户和计算机都能够读写共享的警报文件夹。如果该文件夹所在的计算机运行的操作系统是 Windows NT，则您还应正确配置一个空的会话共享。详细说明，请参阅操作系统文档。

3 配置警报管理器以监控集中警报文件夹的活动。为此：

   a 从 “**警报管理器属性**”对话框中选择 “**集中警报**”选项卡。

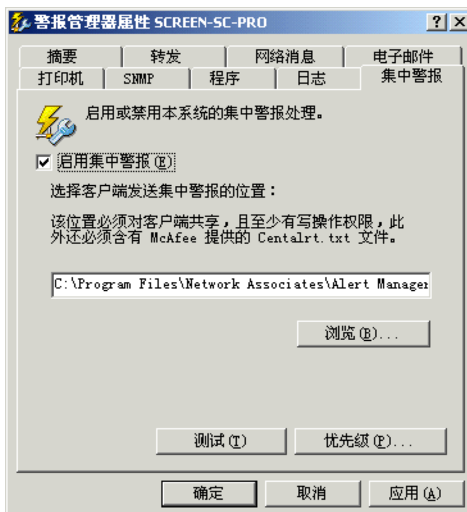


图 **6-25.** 集中警报属性

b 选择 “**启用集中警报**”。

c 键入警报文件夹的位置，或者单击 “**浏览**” 在服务器或网络中查找文件夹。该文件夹必须与客户端防病毒软件使用的用于集中警报的文件夹相同。（请参阅步骤 1）。警报文件夹的默认位置是：

C:\Program Files\Network Associates\Alert Manager\Queue\。

4 单击“**优先级**”指定接收者的计算机要接收的警报消息类型。请参阅第 124 页的 “为接收者设置警报优先级”。

5 单击“**测试**”向接收者的计算机发送一条测试消息。请参阅第 123 页的“发送测试消息”。

6 单击 “**确定**” 保存集中警报设置并返回到 “**警报管理器属性**” 对话框。

自定义警报消息

警报管理器附带多种警报消息，几乎可满足在网络中检测到病毒时所遇到的各类情况要求。警报消息包括预设的优先级、用来识别感染病毒文件和系统的系统变量、感染的病毒以及用来快速、全面查看情况的其他信息。

为满足您的需要，您可以启用或禁用个别的警报消息，也可以更改任何消息的内容及优先级。但由于警报管理器主要针对特殊触发事件激活警报消息，因此当编辑警报消息时，应尽量保留其主要含义。

使用 “**警报管理器消息**” 对话框自定义警报消息。请参阅第 118 页的 “配置警报管理器”来了解如何访问 “**警报管理器消息**” 对话框的详细说明。

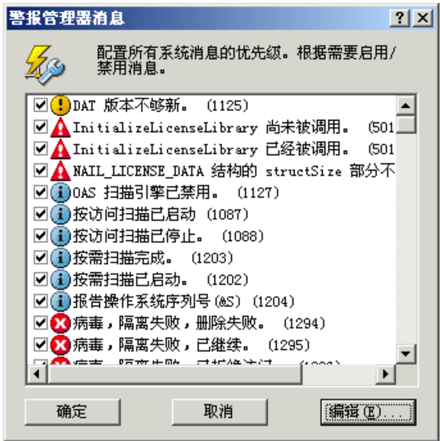


图 **6-26.** 警报管理器消息

现在，您可以执行如下操作之一：

- 启用和禁用警报消息 .
- 编辑警报消息 .

启用和禁用警报消息

尽管在防病毒软件发现病毒或者几乎对其常规操作的所有方面都进行了明显改动时，VirusScan Enterprise 会发送警报消息，但您也许并不希望接收所有警报消息。使用 **“警报管理器消息”** 对话框可以禁用不希望接收的警报消息。

列在 **“警报管理器消息”** 对话框中的每个警报的旁边都有一个复选框。选择此框，表示启用该警报。如果不选择，就表示禁用。默认设置为启用所有可用的警报消息。

启用或禁用警报消息：

1 根据您要启用还是禁用警报消息，选择或取消选择相应的复选框。

2 单击 **“确定”** 保存所做的更改并关闭 **“警报管理器消息”** 对话框。

编辑警报消息

下面列出了两种编辑警报消息的方式：

- 更改警报优先级。
- 编辑警报消息文本。

更改警报优先级

警报管理器从您的客户端防病毒软件接收的某些警报要求您更及时地反应和处理。根据大多数系统管理员分配的紧急程度，系统为每个警报消息都设定了默认的优先级。您可以重新指定这些优先级，以满足自己的需要。使用这些优先级可以过滤警报管理器向接收者发送的消息，这样，接收者就可以首先处理最重要的消息。

更改分配给警报消息的优先级：

1 在 **“警报管理器消息”** 对话框（请参阅第 146 页的 “自定义警报消息”）中，通过单击来选择消息列表中的一个消息。

2 单击 **“编辑”** 打开 **“编辑警报管理器消息”** 对话框。



图 **6-27.** 编辑警报消息的优先级和文本

3 从 **“优先级”** 列表中选择一个优先级。可以为每个警报消息分配 **“关键”**、**“主要”**、**“次要”**、**“警告”** 或 **“信息”** 优先级。

“**警报管理器消息**”对话框中列出的每个消息的旁边都有一个图标，用来识别当前分配给该消息的优先级。每个图标都对应于 “**优先级**”下拉列表中的一个选择。优先级包括：

关键。表示无法清除、隔离或删除防病毒软件检测到的文件病毒。

主要。表示成功地检测和清除了病毒或可能导致防病毒软件停止运行的严重错误和问题。例如 “已删除感染病毒的文件”、“未安装指定产品的许可”或 “内存不足！ ”

次要。表示比主要消息程度轻的检测或状态消息。

警告。表示比通知消息更严重的状态消息。经常与防病毒扫描过程中遇到的非关键问题相关。

信息。表示标准状态和通知消息，例如“已开始按访问扫描”或“扫描已完成，未发现病毒。”

重新指定消息的优先级之后，该消息旁边的图标将发生变化，显示新的优先级状态。

4 单击 “**确定**”。

按优先级过滤消息

要过滤消息，请配置在警报管理器中设置的每种警报方法，以便只接收某个优先级的消息。例如，假设需要客户端防病毒软件在网络上查找到病毒时要求警报管理器呼叫您，但是不需要它发送日常事务运行消息。为此，您需要为病毒警报指定关键或主要优先级，并为日常事务通知性消息指定次要或警告优先级。然后，配置警报管理器，使其只将较高的优先级消息发送到寻呼机的电子邮件地址。

有关为特定接收者应用优先级过滤规则的说明，请参阅第 124 页的“为接收者设置警报优先级”。

编辑警报消息文本

为了帮助您对需要注意的情况做出响应，警报管理器在其消息中包括了足够的信息，以识别问题的来源以及问题环境的相关信息。您可以根据需要编辑消息文本。例如，可以向警报消息添加评论，以便更详细地描述问题或列出技术支持的联系信息。

> **注释**
>
> 尽管可以编辑警报消息文本以表达您自己的想法，但仍应尽量保留主旨，原因在于警报管理器只有在遇到某些具体情况时才发送相应的消息。例如，只有当警报管理器实际开始某项工作时才会发送 “任务已启动”警报。

编辑警报消息文本：

1. 单击 “**警报管理器消息**”对话框中列表中的一条消息以选择它。
2. 单击 “**编辑**”打开 “**编辑警报管理器消息**”对话框。
3. 您可以根据需要编辑消息文本。文本包括在百分号中，例如 `%COMPUTERNAME%`，它代表一个变量，警报管理器会在生成警报消息时用文本来替换这部分。请参阅第 150 页的 “使用警报管理器系统变量”。
4. 单击 “**确定**”保存更改并返回到 “**警报管理器**”对话框。

使用警报管理器系统变量

警报管理器 4.7 包含在警报消息文本中使用的系统变量。这些变量指的是系统功能，例如系统日期和时间、文件名或计算机名称。在发送警报通知时，警报管理器会动态使用特定的值来替换这个变量。

例如，列在“**警报管理器消息**”对话框中的主要警报“已成功清除感染病毒的文件 (1025)”默认设置如下：

> 文件 %FILENAME% 感染了 %VIRUSNAME% %VIRUSTYPE%。使用 %ENGINEVERSION% 版扫描引擎和 %DATVERSION% 版 DAT，已将该文件感染病毒成功清除。

如果这个警报是从防病毒应用程序发送到警报管理器，警报管理器会动态地对系统变量赋予真值，例如将 `%FILENAME%` 变量赋值为 `MYDOCUMENT.DOC`。

最常用的一些系统变量为：

`%DATVERSION%`	生成警报的防病毒软件当前使用的 DAT 文件版本。
`%ENGINEVERSION%`	防病毒软件当前使用的用于检测病毒感染或其他问题的防病毒引擎版本。
`%FILENAME%`	文件的名称。可包括发现的感染病毒文件的名称或者从扫描操作中排除的文件的名称。
`%TASKNAME%`	活动任务名称，如按访问扫描或 VirusScan Enterprise 7.0 的自动更新任务。警报管理器可以使用该选项来报告发现病毒的那个任务的名称或者在扫描操作中报告出错的那个任务的名称。
`%VIRUSNAME%`	感染的病毒名称。
`%DATE%`	运行警报管理器的计算机的系统日期。
`%TIME%`	运行警报管理器的计算机的系统时间。
`%COMPUTERNAME%`	计算机在网络上的名称。可包含感染病毒的计算机、报告设备驱动程序错误的计算机以及受该程序影响的任何其他计算机。
`%SOFTWARENAME%`	可执行文件的名称。可包含检测病毒的应用程序、报告出错的应用程序或者受该程序影响的任何其他应用程序。
`%SOFTWAREVERSION%`	从活动软件包中取得的版本号。可包含检测病毒的应用程序、报告出错的应用程序或者受该程序影响的任何其他应用程序。
`%USERNAME%`	当前登录到服务器的用户登录名。例如，它可以告诉您是否有人取消了扫描操作。

警告

若消息文本中包含系统变量，但该变量可能不被生成警报信息的事件使用，那么在编辑该消息文本时要当心。若在警报中使用系统变量，但警报实际上却不使用系统变量字段，会导致无法预料的结果，包括意义混乱的消息文本，甚至会出现系统崩溃。

下面列出了可在警报管理器消息中使用的所有警报管理器系统变量：

- %ACCESSPROCESSNAME%
- %CLIENTCOMPUTER%
- %COMPUTERNAME%
- %DATVERSION%
- %DOMAIN%
- %ENGINESTATUS%
- %ENGINEVERSION%
- %EVENTNAME%
- %FILENAME%
- %GMTDAY%
- %GMTHOUR%
- %GMTMIN%
- %GMTMONTH%
- %GMTSEC%
- %GMTTIME%
- %GMTYEAR%
- %INFO%
- %MAILIDENTIFIERINFO%
- %MAILSUBJECTLINE%
- %MAILTONAME%
- %NOTEID%
- %NOTESDBNAME%
- %NOTESSERVERNAME
- %LANGUAGECODE%
- %LOCALDAY%
- %LOCALHOUR%
- %LOCALMIN%
- %LOCALMONTH%
- %LOCALSEC%
- %LOCALTIME%
- %LOCALYEAR%
- %LONGDESCRIPT%
- %MAILCCNAME%
- %MAILFROMNAME%
- %NUMCLEANED%
- %NUMDELETED%
- %NUMQUARANTINED%
- %NUMVIRS%
- %OBRULENAME%
- %OS%
- %PROCESSORSERIA%
- %RESOLUTION%
- %SCANRETURNCODE%
- %SEVERITY%
- %SHORTDESCRIPT%
- %SOFTWARENAME%
- %SOFTWAREVERSION%
- %SOURCEIP%
- %SOURCEMAC%
- %SOURCESEG%
- %TARGETCOMPUTERNAME%
- %TARGETIP%
- %TARGETMAC%
- %TASKID%
- %TASKNAME%
- %TRAPID%
- %TSCLIENTID%
- %URL%
- %USERNAME%
- %VIRUSNAME%
- %VIRUSTYPE%

更新 7

VirusScan Enterprise 软件根据病毒定义 (DAT) 文件中的信息识别病毒。如果没有更新后的文件，本软件将无法检测新病毒变种或作出有效响应。某些不使用最新 DAT 文件的软件可能对您的防病毒程序构成威胁。

新病毒以每月 500 多个的速度不断涌现。为迎接这一挑战， McAfee 每周会发布新的 DAT 文件，并使用最新的研究成果来识别新病毒或病毒变种的特征。 VirusScan Enterprise 软件附带的更新任务能够帮助您轻松地充分利用这项服务。

我们已经改进了自动更新功能，因此更新过程变得更容易和更灵活。这一功能允许您使用立即更新或计划更新功能同时下载最新的DAT文件、扫描引擎和EXTRA.DAT。您也可以借助该功能下载 Hotfix 和产品升级。

这部分包含下列主题：

更新策略

有许多可用于更新的方法。您可以使用更新任务、手动更新、登录脚本或管理工具的计划更新。本文档将讨论使用自动更新及手动更新。其他方法在本文档中则没有述及。

高效的更新策略通常需要至少一个您公司的客户机或服务器来从 Network Associates 下载站点获取更新。通过该客户机或服务器，可在整个公司的范围内复制文件，提供对所有其他计算机的的访问。理想情况下，您可将更新文件自动复制到共享节点，而且使得在您网络中传输的数据量最小化。

高效更新要考虑的主要因素是客户机以及站点的数量。也可能会有其他因素影响您的更新方案，例如每个远程站点的系统数量以及远程站点访问 Internet 的方式。但是向您共享节点的复制以及计划更新的基本概念适用于任意规模的公司。

若使用更新任务进行更新，您可：

- 根据自己的方便在整个网络范围内确定DAT文件转出和产品升级的时间，并使管理员或网络用户的必要干预尽可能少。例如，您可以将更新任务错开，或者设置一个计划，在网络的不同部分分时段或轮流进行 DAT 文件更新和产品升级。
- 在不同的服务器和域控制器之间、广域网的不同区域之间或其他网段之间分别执行转出管理任务。将更新网络流量主要限制在内部还可以减少潜在的网络安全缺口。
- 减少不得不等待下载新的 DAT 或升级文件的可能性。McAfee 计算机上的通讯流量在定期发布 DAT 文件和推出新版本的产品时会显著增长。避免网络带宽过于繁忙可以将您在部署新软件时中断的可能性降到最低。

自动更新

该版本的 VirusScan Enterprise 使用自动更新 7.0 组件来计划任务和执行更新功能。

- 自动更新 7.0 计划功能可用于计划所有任务，包括按需、更新和镜像任务。更多信息，请参阅第 176 页的 “计划任务”。
- 自动更新 7.0 更新功能用于执行计划的或立即更新任务。您可以更新 DAT 文件、扫描引擎、补丁程序、 EXTRA.DAT 及产品升级。

VirusScan Enterprise 产品附带默认的更新任务，该任务计划于每周五下午 5:00 进行更新，一个小时的随机性。该默认更新任务叫做 “**自动更新**”。您可以重新命名并配置该默认的“**自动更新**”任务。您也可以创建其他更新任务以满足您的更新需要。

下列更新任务是可恢复性的：

- **从 HTTP、UNC 或本地站点更新的任务**。如果更新任务由于某种原因在更新过程中被打断，更新任务会在下次启动时从中断处继续运行。

- **从 FTP 站点更新的任务**。如果某个文件在下载过程中中断，则任务不可恢复。但是，如果任务是下载多个文件，而任务中断，那么该任务会恢复中断时正在下载的文件之前的文件。

这部分包含下列主题：

- 创建自动更新任务
- 配置自动更新任务
- 运行自动更新任务
- 查看活动日志

创建自动更新任务

创建新的自动更新任务：

1. 打开 “**VirusScan 控制台**”。有关说明，请参阅第 18 页的 “VirusScan 控制台”。
2. 使用以下方法之一创建新的更新任务：
   - 无需选择任务列表中的项目，只要右键单击控制台中的空白区域，然后选择 “**新建更新任务**”。
   - 选择 “**任务**”菜单中的 “**新建更新任务**”。

   在 “**VirusScan 控制台**”任务列表中将突出显示新的更新任务。
3. 接受默认的任务名称或者键入新名称，然后按 ENTER 键打开“**自动更新属性**”对话框。有关详细的配置信息，请参阅 “配置自动更新任务”。

配置自动更新任务

为满足您自己的需求，您可以配置和计划自动更新任务。

1. 打开 “**VirusScan 控制台**”。有关说明，请参阅第 18 页的 “VirusScan 控制台”。
2. 用这些方法之一打开 “**自动更新属性**”对话框：
   - 突出显示控制台任务列表中的任务，然后从 “**任务**”菜单中选择 “**属性**”。
   - 双击任务列表中的任务。
   - 右键单击任务列表中的任务，然后选择 “**属性**”。
   - 突出显示任务列表中的任务，然后单击 。



图 **7-1.** 自动更新属性 **-** 新建更新任务

注释
在您 “**计划**”更新任务或执行 “**立即更新**”任务之前，要先配置更新任务。

3 在 “**日志文件**”区域，从下列选项中选择：

- **记录到文件**。在日志文件中记录更新活动。
- 接受该文本框中默认的日志文件名称和位置，或者输入其他日志文件名称和位置，或者单击 “**浏览**”查找合适的位置。

注释
默认情况下，日志信息被记录在位于以下目录中的 UPDATELOG.TXT 文件中：

< 驱动器 >:Winnt\Profiles\All Users\Application Data\Network Associates\Virusscan

4 在 “**运行选项**”区域中，您可以指定要在**自动更新**任务结束后启动的可执行文件。例如，您可使用该选项启动一个网络邮件实用程序来通知管理员更新操作已成功完成。

- **请输入更新完成后运行的可执行文件**。输入要运行的可执行文件的路径，或单击 “**浏览**”进行查找。
- **仅在成功更新后运行**。仅当更新成功后运行可执行程序。如果更新不成功，则所选的程序不会运行。

注释
当前登录的用户必须能够执行您指定的程序文件。如果当前登录的用户无权访问含有该程序文件的文件夹或当前无用户登录，该程序也不会运行。

5 单击“**计划**”以计划更新任务。更多信息，请参阅第 175 页的 “计划任务”。

6 单击 “**应用**”保存更改。

7 如果希望立即运行更新任务，请单击 “**立即更新**”。

8 单击 “**确定**”关闭 “**计划设置**”对话框。

> **注释**
> 更新任务使用自动更新资料库列表中的配置设置来进行更新。更多信息，请参阅第 163 页的 “自动更新资料库列表”。

运行自动更新任务

一旦通过所需的更新属性配置了您的任务，就可以运行更新任务。这部分包含下列主题：

- 运行该更新任务
- 更新任务执行过程中的更新活动

运行该更新任务

1 打开 “**VirusScan 控制台**”。有关说明，请参阅第 18 页的 “VirusScan 控制台”。

2 使用以下方法之一运行更新任务：

- **按计划更新**。如果计划了更新任务，则该任务可以在无人值守的情况下运行。

> **注释**
> 计算机必须处于开机状态，更新任务才能运行。如果系统在计划任务开始运行时处于关机状态，那么这项任务将在计算机处于开机状态时的下一个计划时间运行，或者，如果选择了 “**计划**”选项卡中 “**计划设置**”上的 “**运行错过的任务**”选项，这项任务将在计算机启动时开始。

- **立即更新**。立即启动更新任务的方法有三种：
  - 用于默认更新任务的立即更新命令。
  - 所有更新任务的开始命令。
  - 用于所有更新任务的立即更新命令。

用于默认更新任务的立即更新命令

使用 “**立即更新**”立即启动默认的更新任务。

> **注释**
> “**立即更新**”仅对在安装本产品时创建的默认更新任务有效。您可以重命名和重新配置默认的更新任务，但如果删除了该默认任务，“**立即更新**”将随即被禁用。

1. 打开 “**VirusScan 控制台**”。有关说明，请参阅第 18 页的 “VirusScan 控制台”。
2. 按照以下方法之一，使用 “**立即更新**” 执行立即更新：
   - 在 “**VirusScan 控制台**” 中，选择 “**任务**” 菜单中的 “**立即更新**”。
   - 右键单击系统任务栏中的 ，然后选择 “**立即更新**”。
   - 该任务结束后，单击 “**关闭**” 退出 “**McAfee 更新程序**” 对话框，或等待窗口自动关闭。

所有更新任务的开始命令

您可使用 “**VirusScan 控制台**” 中的 “**开始**” 来立即启动任意更新任务。

1. 打开 “**VirusScan 控制台**”。有关说明，请参阅第 18 页的 “VirusScan 控制台”。
2. 按照以下方法之一，从 “**VirusScan 控制台**” 启动立即更新：
   - 突出显示控制台任务列表中的任务，然后从 “**任务**” 菜单中选择 “**开始**”。
   - 右键单击任务列表中的任务，然后选择 “**开始**”。
   - 突出显示任务列表中的任务，然后单击 。
   - 该任务结束后，单击 “**关闭**” 退出 “**McAfee 更新程序**” 对话框，或等待窗口自动关闭。

用于所有更新任务的立即更新命令

您可使用 “**自动更新属性**” 对话框中的 “**立即更新**” 来立即启动任意更新任务。

1. 打开 “**VirusScan 控制台**”。有关说明，请参阅第 18 页的 “VirusScan 控制台”。
2. 打开选定的更新任务的 “**自动更新属性**” 对话框。有关打开 “**自动更新属性**” 对话框的详细信息，请参阅第 155 页的 “配置自动更新任务”。
3. 单击 “**自动更新属性**” 对话框中的 “**立即更新**”。
4. 该任务结束后，单击 “**关闭**” 退出 “**McAfee 更新程序**” 对话框，或等待窗口自动关闭。

更新任务执行过程中的更新活动

使用自动更新 7.0 组件的产品从下载资料库中下载 CATALOG.Z 文件。CATALOG.Z 文件用于已更新文件的增量更新。

查看活动日志

更新任务活动日志显示了更新操作的详细信息。例如，它显示了更新后的 DAT 文件和引擎版本号。

查看活动日志：

1 打开 “**VirusScan 控制台**”。有关说明，请参阅第 18 页的 “VirusScan 控制台”。

2 使用以下方法之一，打开活动日志文件：

   - 突出显示任务，然后选择 “**任务**” 菜单中的 “**活动日志**”。
   - 右键单击任务列表中的任务，并选择 “**查看日志**”。

3 要关闭活动日志，请选择 “**文件**” 菜单中的 “**退出**”。

镜像任务

镜像任务允许您从资料库列表中所定义的第一个可访问的下载资料库下载更新文件，并将文件下载到您网络中的镜像站点。每个镜像站点都复制了包含更新文件的 Network Associates 站点。然后，网络中的计算机就可以从这个镜像站点下载这些文件。这种方法非常实用，原因在于，无论网络中的计算机是否具有 Internet 访问权，都可以对其进行更新，并且由于您的计算机是在与比 Network Associates 的 Internet 站点更近的服务器通讯，因此可以节省访问和下载时间，所以这种方法更为有效。该任务最见的用途是将 Network Associates 下载站点的内容镜像到本地服务器。

这部分包含下列主题：

- 创建镜像任务
- 运行镜像任务
- 查看镜像任务活动日志

创建镜像任务

为需要的每个镜像位置创建镜像任务：

创建新的镜像任务：

1 打开 “**VirusScan 控制台**”。有关说明，请参阅第 18 页的 “VirusScan 控制台”。

2 使用以下方法之一创建镜像任务：

   - 无需选择任务列表中的项目，只要右键单击控制台中的空白区域，然后选择 “**新建镜像任务**”。
   - 选择 “**任务**” 菜单中的 “**新建镜像任务**”。

在 “**VirusScan 控制台**”任务列表中将突出显示新的镜像任务。

3 接受默认的任务名称或者键入新名称，然后按 ENTER 键打开“**自动更新属性**”对话框。有关详细的配置信息，请参阅第 160 页的 “配置镜像任务”。

配置镜像任务

为满足您的需要，您可以配置和计划镜像任务。

1 打开 “**VirusScan 控制台**”。有关说明，请参阅第 18 页的 “VirusScan 控制台”。

2 用这些方法之一打开 “**自动更新属性**”对话框：

- 突出显示控制台任务列表中的任务，然后从 “**任务**”菜单中选择 “**属性**”。
- 双击任务列表中的任务。
- 右键单击任务列表中的任务，然后选择 “**属性**”。
- 突出显示任务列表中的任务，然后单击 。



图 **7-2.** 自动更新属性 **-** 新建镜像任务

注释
在您 “**计划**”镜像任务或执行 “**立即镜像**”任务之前，要先配置镜像任务。

3 在 “**日志文件**”区域，从下列选项中选择：

- **记录到文件**。在日志文件中记录镜像更新活动。
- 接受该文本框中默认的日志文件名称和位置，或者输入其他日志文件名称和位置，或者单击 “**浏览**”查找合适的位置。

注释
在默认情况下，日志信息被被写入位于以下目录下的 VSEMIRRORLOG.TXT 文件中：

< 驱动器 >:Winnt\Profiles\All Users\Application Data\Network Associates\Virusscan

4 单击 “**镜像位置**” 打开 “**镜像位置设置**” 对话框。

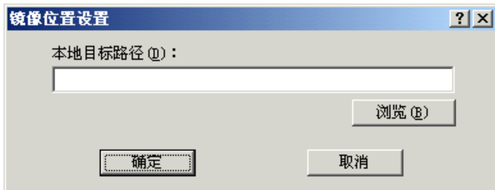


图 7-3. 镜像位置设置

a 输入本地系统上用于镜像站点的目标路径，或单击 “**浏览**” 查找所需位置。

b 单击 “**确定**” 返回到 “**自动更新属性**” 对话框。

5 在 “**运行选项**” 区域中，您可指定在**镜像**任务结束后启动的可执行文件。例如，您可使用该选项启动一个网络邮件实用程序来通知管理员更新操作已成功完成。

- **请输入镜像完成后运行的可执行文件**。输入要运行的可执行文件的路径，或单击 “**浏览**” 进行查找。
- **仅在成功镜像后运行**。仅当更新成功后运行可执行程序。如果更新不成功，则所选的程序不会运行。

注释
当前登录的用户必须能够执行您指定的程序文件。如果当前登录的用户无权访问含有该程序文件的文件夹或当前无用户登录，该程序也不会运行。

6 单击 “**计划**” 以计划镜像任务。关于计划任务的说明，请参阅第 175 页的 “计划任务”。

7 单击 “**应用**” 保存更改。

8 如果希望立即运行镜像任务，请单击 “**立即镜像**”。

9 单击 “**确定**” 关闭 “**计划设置**” 对话框。

注释
“**镜像**” 任务使用资料库列表中的配置设置来执行更新。更多信息，请参阅第 163 页的 “自动更新资料库列表”。

运行镜像任务

一旦通过所需的属性配置完镜像任务，就可以使用以下方法之一运行镜像任务：

- **按计划镜像**。如果计划了镜像任务，则它可以在无人值守的情况下运行。

  注释
  计算机必须处于开机状态，镜像任务才能运行。如果系统在计划任务开始运行时处于关机状态，那么这项任务将在计算机处于开机状态时的下一个计划时间运行，或者，如果选择了 “**计划**” 选项卡中 “**计划设置**” 上的 “**运行错过的任务**” 选项，这项任务将在计算机启动时开始。

- **立即镜像**。立即启动镜像任务的方法有两种：
  - 用于镜像任务的开始命令
  - 用于镜像任务的立即镜像命令

用于镜像任务的开始命令

您可使用 “**VirusScan 控制台**” 中的 “**开始**” 来立即启动任意镜像任务。

1. 打开 “**VirusScan 控制台**”。有关说明，请参阅第 18 页的 “VirusScan 控制台”。
2. 按照以下方法之一，从 “**VirusScan 控制台**” 启动立即镜像更新：
   - 突出显示控制台任务列表中的任务，然后从 “**任务**” 菜单中选择 “**开始**”。
   - 右键单击任务列表中的任务，然后选择 “**开始**”。
   - 突出显示任务列表中的任务，然后单击 ▷ 。
   - 该任务结束后，单击 “**关闭**” 退出 “**McAfee 更新程序**” 对话框，或等待窗口自动关闭。

用于镜像任务的立即镜像命令

您可使用 “**自动更新属性**” 对话框中的 “**立即镜像**” 来立即启动任意镜像任务。

1. 打开 “**VirusScan 控制台**”。有关说明，请参阅第 18 页的 “VirusScan 控制台”。
2. 打开选定的镜像任务的 “**自动更新属性**” 对话框。有关打开 “**自动更新属性**” 对话框的详细信息，请参阅第 160 页的 “配置镜像任务”。
3. 单击 “**自动更新属性**” 对话框中的 “**立即镜像**”。
4. 该任务结束后，单击 “**关闭**” 退出 “**McAfee 更新程序**” 对话框，或等待窗口自动关闭。

查看镜像任务活动日志

镜像任务活动日志显示了更新操作的详细信息。例如，它显示了更新后的 DAT 文件和引擎版本号。

1 打开 “**VirusScan 控制台**”。有关说明，请参阅第 18 页的 “VirusScan 控制台”。

2 使用以下方法之一，打开活动日志文件：

   - 突出显示任务，然后选择 “**任务**”菜单中的 “**活动日志**”。
   - 右键单击任务列表中的任务，并选择 “**查看日志**”。

3 要关闭活动日志，请选择 “**文件**”菜单中的 “**退出**”。

自动更新资料库列表

您可以使用自动更新资料库列表下载最新的 DAT 文件更新、扫描引擎升级、HotFix 和 / 或产品升级。

自动更新资料库列表中指定了执行更新任务所需的资料库和配置信息。例如：

- 更新资料库信息和位置。
- 代理服务器信息。
- 客户机的登录证书，用来访问资料库并检索更新。

VirusScan Enterprise 软件有两个资料库列表，用于配置从以下站点下载：

```
ftp://ftp.nai.com/commonupdater
http://download.nai.com/products/commonupdater
```

如果您在独占使用VirusScan Enterprise 7.0，或者在一个复杂的环境中将VirusScan Enterprise 7.0 与 VirusScan 4.5.1 或 NetShield 4.5 一起使用，可以使用其中一个站点下载最新的更新。

FTP 资料库是默认的站点。HTTP 资料库是备用站点。如果您采用系统配置来使用自动更新资料库列表，则更新任务将试图从 FTP 站点首先下载。如果从 FTP 站点更新失败，它会尝试从 HTTP 站点下载。您可以移动列表中的站点，更改配置，或者移除 FTP 和 HTTP 这两个站点或其中一个。

如果希望导入自定义的自动更新资料库列表，请指定获取软件的源资料库，或者使用可以从主库复制的多个更新位置，但您必须配合 VirusScan Enterprise 应用 McAfee AutoUpdate Architect™ 实用程序。更多信息，请参阅《McAfee AutoUpdate Architect 产品指南》。

这部分包含下列主题：

- 导入自动更新资料库列表
- 编辑自动更新资料库列表

导入自动更新资料库列表

要从其他位置导入自动更新资料库列表：

1 打开 “**VirusScan 控制台**”。有关说明，请参阅第 18 页的 “VirusScan 控制台”。

2 选择 “**工具**” | “**导入自动更新资料库列表**”。

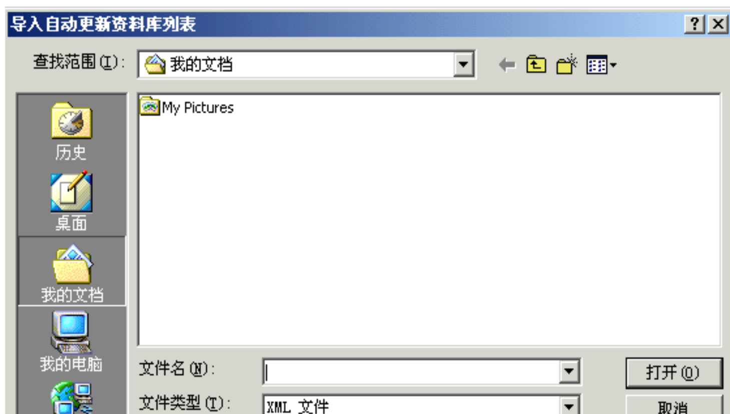


图 7-4. 导入自动更新资料库列表

3 在 “**查找范围**” 框中，输入 .XML 文件的位置，或单击 ▼ 找到这个位置，然后选择该文件。

4 单击 “**打开**” 导入自动更新资料库列表。

编辑自动更新资料库列表

使用 “**编辑站点列表**” 对话框，向列表中添加新的自动更新资料库并配置、编辑和删除现有的资料库以及组织该列表中的资料库。

这部分包含下列主题：

- 添加并编辑自动更新资料库
- 删除和重新组织资料库
- 指定代理服务器设置

添加并编辑自动更新资料库

可从该对话框将自动更新资料库添加到列表中。您也可以使用McAfee AutoUpdate Architect™ 创建资料库并将其导出到 VirusScan Enterprise。关于使用 McAfee AutoUpdate Architect 创建并导出资料库的详细信息，请参阅 《McAfee AutoUpdate Architect 产品指南》。

自动更新资料库的状态可以为已禁用或已启用。每个资料库还可以为其他状态，即备用或只读状态。

- 如果其他自动更新资料库均不可用，则可以使用备用资料库进行更新。备用资料库总是被列在列表的最底部。默认情况下， Network Associates HTTP 下载站点即是备用资料库。
- 只读资料库不可编辑。只有在创建资料库时使用的是 McAfee AutoUpdate Architect™ 时，列表中只读资料库才可见。

注释
McAfee AutoUpdate Architect 实用程序还可隐藏资料库使其不显示在 VirusScan Enterprise 自动更新资料库列表中。

在自动更新资料库列表中添加或编辑资料库：

1. 打开 “**VirusScan 控制台**”。有关说明，请参阅第 18 页的 “VirusScan 控制台”。
2. 选择 “**工具**” | “**编辑自动更新资料库列表**”。



图 7-5. 编辑自动更新资料库列表 - 资料库选项卡

3. 选择“**资料库**”选项卡。FTP 资料库是默认的站点。HTTP 资料库是备用站点。
4. 要添加或编辑自动更新资料库列表，请从下列操作中选择：
   - 要添加资料库，请单击 “**添加**” 打开 “**资料库设置**” 对话框。

- 要编辑资料库，请在 “**资料库描述**” 列表中将其突出显示，然后单击 “**编辑**” 打开 “**资料库设置**” 对话框。

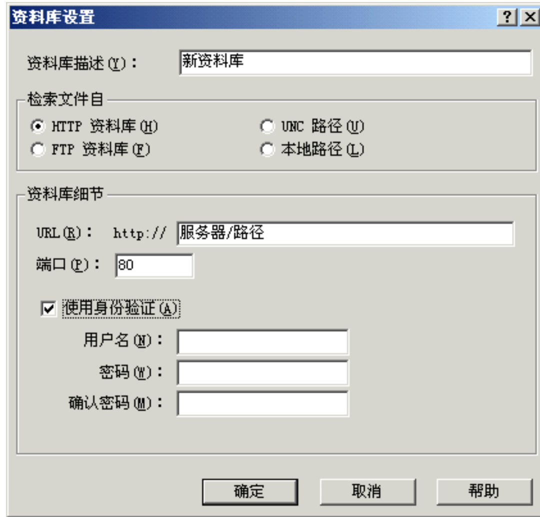


图 7-6. 资料库设置

5 在 “**资料库描述**” 框中，输入该资料库的名称或说明。

6 在 “**检索文件自**” 区域中，从下列选项中选择资料库类型或路径：

- **HTTP资料库**。该选项为默认选项。使用您在下面指定的HTTP资料库位置作为您检索更新文件的资料库。
- **FTP资料库**。使用您在下面指定的FTP资料库位置作为您检索更新文件的资料库。
- **UNC 路径**。使用您在下面指定的 UNC 路径作为您检索更新文件的资料库。
- **本地路径**。使用您在下面指定的本地站点作为您检索更新文件资料库。

7 在 “**资料库细节**” 区域中，能够输入的信息取决于您在 “**检索文件自**” 区域中选择的资料库类型或路径。从以下选项中进行选择：

- 如果您选择了 “**HTTP 资料库**” 或 “**FTP 资料库**”，请参阅第 166 页的 “HTTP 或 FTP 资料库详细信息”以获取详细说明。
- 如果您选择了 “**UNC 路径**” 或 “**本地路径**”，请参阅第 168 页的 “UNC 路径或本地路径资料库详细信息”以获取详细说明。

HTTP 或 FTP 资料库详细信息

如果您选择了 HTTP 或 FTP 资料库，请执行这些步骤。

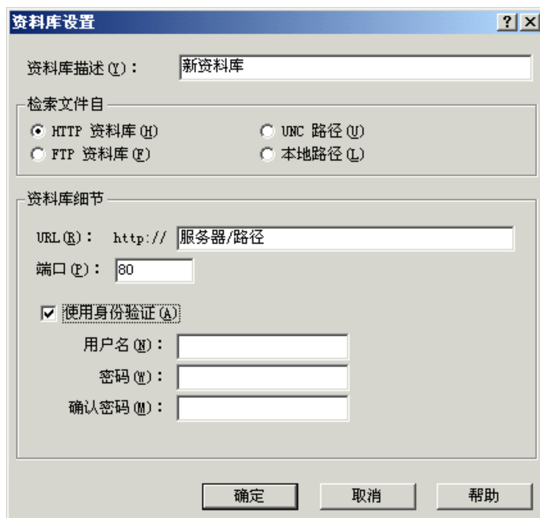


图 7-7. 资料库详细信息 -HTTP 或 FTP 站点

1 在 “**资料库细节**”区域中，输入您所选定的资料库路径和端口号，并指定访问该资料库的安全证书。

- **URL**。输入 HTTP 路径或 FTP 资料库位置，如下：
  - **HTTP**。输入 HTTP 服务器和更新文件所在目录的位置。DAT 文件更新默认的 McAfee HTTP 资料库位于：

    `http://download.nai.com/products/commonupdater`

  - **FTP**。输入 FTP 服务器和更新文件所在目录的位置。DAT 文件更新默认的 McAfee FTP 资料库位于：

    `ftp://ftp.nai.com/commonupdater`

- **端口**。输入您选择的 HTTP 或 FTP 服务器的端口号。
- **使用身份验证**或**使用匿名登录**。标题的区别取决于您是否选择了 HTTP 路径或 FTP 路径。指定访问该资料库的安全证书。然后输入“**用户名**”、“**密码**”和 “**确认密码**”。

2 单击 “**确定**”保存更改并返回到 “**编辑自动更新资料库列表**”对话框。

UNC 路径或本地路径资料库详细信息

如果选择了 UNC 或本地路径，请执行这些步骤。

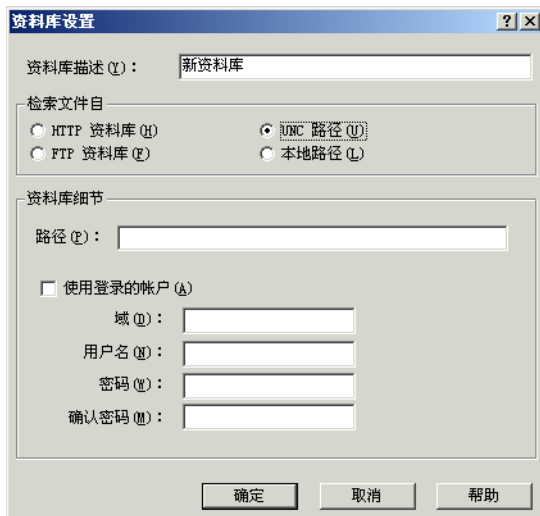


图 **7-8.** 资料库详细信息 **-UNC** 或本地路径

1 在 “**资料库细节**”区域中，输入您所选资料库的路径，并确定是否使用已登录的帐户或通过指定用户名和密码来加强安全性。

- **路径**。输入要从哪个路径位置检索更新文件。
  - **UNC 路径**。使用 UNC 符号（\\ 服务器名称 \ 路径）输入更新文件所在的资料库路径。
  - **本地路径**。输入更新文件所在的本地文件夹的路径，或者单击 “**浏览**”查找该文件夹。
- **使用登录的帐户**。确定要使用哪个帐户。请从以下选项中选择：
  - 要使用当前登录的帐户，请选择 “**使用登录的帐户**”。
  - 取消选择“**使用登录的帐户**”以使用另一个帐户，则请输入“**域**”、“**用户名**”和 “**密码**”，及 “**确认密码**”。

2 单击 “**确定**”保存更改并返回到 “**编辑自动更新资料库列表**”对话框。

删除和重新组织资料库

要删除或重新组织资料库列表中的资料库，请执行以下步骤：

1 打开 “**VirusScan 控制台**”。有关说明，请参阅第 18 页的 “VirusScan 控制台”。

2 选择 “**工具**” | “**编辑自动更新资料库列表**”。



图 7-9. 编辑自动更新资料库列表 - 资料库选项卡

3 选择 “**资料库**” 选项卡。

4 要删除或重新组织资料库列表中的资料库，请从下面的操作中选择：

- 要删除一个资料库，请在列表中突出显示它，然后单击 “**删除**”。
- 要重新组织列表中的资料库，首先突出显示一个资料库，然后反复单击 “**上移**” 或 “**下移**”，直到资料库移到列表中的理想位置为止。

注释
资料库在列表中的排列顺序，就是在更新操作过程中资料库被访问的顺序。

指定代理服务器设置

如果您的网络使用了代理服务器，您可以指定代理服务器要使用的设置、代理服务器地址，并确定是否要使用身份验证。此处配置的代理服务器设置将应用于资料库列表中的所有资料库。

要指定代理服务器设置，请执行以下步骤：

1 打开 “**VirusScan 控制台**”。有关说明，请参阅第 18 页的 “VirusScan 控制台”。

2 选择 “**工具**” | “**编辑自动更新资料库列表**”。

3 选择 “**代理服务器设置**”选项卡。

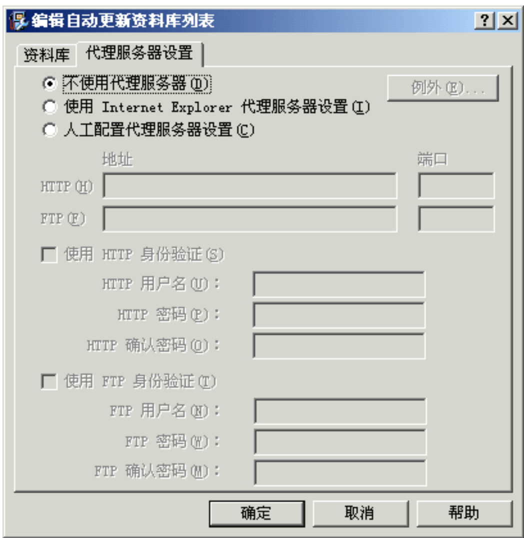


图 **7-10.** 编辑自动更新资料库列表 **-** 代理服务器设置选项卡

4 确定是否要使用代理服务器，如果需要，确定要使用的设置。请从以下选项中选择：

- **不使用代理服务器**。该选项为默认选项。不指定代理服务器。选择该选项，然后单击 “**确定**”保存设置并关闭 “**编辑自动更新资料库列表**”对话框。
- **使用 Internet Explorer 代理服务器设置**。使用当前安装的 IE 版本的代理服务器设置。选择该选项，然后单击 “**确定**”保存设置并关闭 “**编辑自动更新资料库列表**”对话框。
- **人工配置代理服务器设置**。配置代理服务器设置以满足您自己的需求。

选择该选项，然后输入所选资料库的地址、端口和信息，如下所示：

- **HTTP 地址**。输入 HTTP 代理服务器的地址。
- **HTTP 端口**。输入 HTTP 代理服务器的端口号。
- **FTP 地址**。输入 FTP 代理服务器的地址。
- **FTP 端口**。输入 FTP 代理服务器的端口号。

确定是否要为您指定的 HTTP 或 FTP 代理服务器使用身份验证。请从以下选项中选择：

- **使用 HTTP 身份验证**。要加强 HTTP 代理服务器的身份验证功能，请选择该选项，然后输入"**HTTP 用户名**"、"**HTTP 密码**"，及"**HTTP 确认密码**"。
- **使用 FTP 身份验证**。要加强 FTP 代理服务器的身份验证功能，请选择该选项，然后输入"**FTP 用户名**"、"**FTP 密码**"，及"**FTP 确认密码**"。

5 如果要指定代理服务器的例外情况，请单击"**例外**"。如果不想指定例外情况，请跳过这个步骤并转到步骤 6。

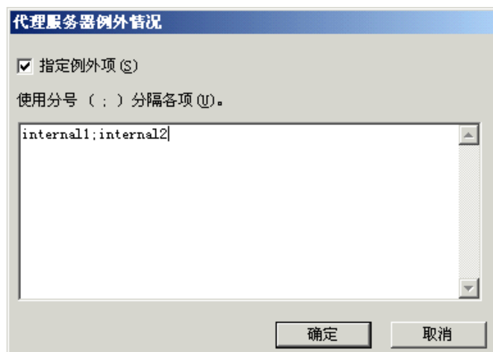


图 7-11. 代理服务器例外情况

a 选择"**指定例外项**"，然后输入例外项，各项之间用分号间隔。

b 单击"**确定**"保存更改并返回到"**代理服务器设置**"选项卡。

6 单击"**确定**"保存更改并关闭"**编辑自动更新资料库列表**"对话框。

回滚 DAT 文件

如果您发现由于某些原因当前的 DAT 文件受到破坏或不兼容，可使用该功能将 DAT 文件回滚为上一个备份版本。无论何时回滚 DAT 文件，有问题的 DAT 版本被存储在资料库中。下一次执行更新时会将资料库中的 DAT 版本与更新资料库中的 DAT 文件进行比较。如果新 DAT 文件与标记为有问题的版本相同，则不执行更新。

要回滚 DAT 文件，请按照以下步骤操作：

1 打开 "**VirusScan 控制台**"。有关说明，请参阅第 18 页的 "VirusScan 控制台"。

2 选择 "**工具**" | "**回滚 DAT**"。"**McAfee 更新程序**" 对话框将打开。

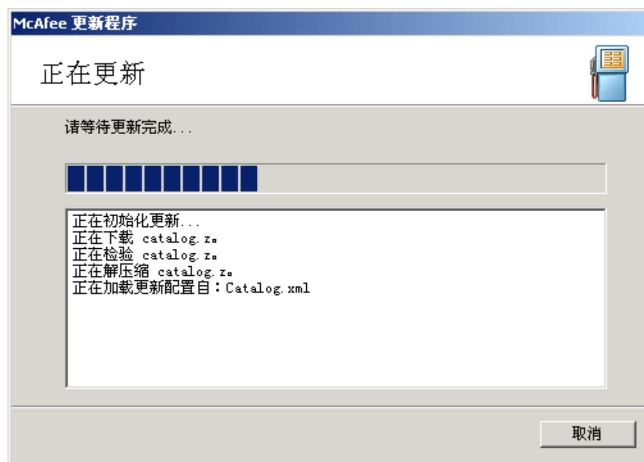


图 7-12. 回滚 **DAT-** 正在更新

3 回滚看起来与更新相同，除了有详细信息显示 "正在执行 DAT 回滚"。回滚结束后，单击 "**关闭**" 退出 "**McAfee 更新程序**" 窗口，或等待窗口自动关闭。

注释
执行回滚时，总是恢复上一个 DAT 文件备份。

手动更新

McAfee 建议您使用 VirusScan Enterprise 软件自带的自动更新任务来安装新版本的 DAT 文件。该实用程序可以为您提供正确更新 DAT 文件的快捷方法。如果您要自行安装 DAT 文件，可从以下更新站点手动下载 DAT 文件：

```
http://www.mcafeeb2b.com/naicommon/download/dats/find.asp
ftp://ftp.nai.com/pub/antivirus/datfiles/4.x
```

- **定期发布的 DAT 文件**。McAfee 将这些文件存储在它的 FTP 站点中，文件名为 DAT-XXX.ZIP，类型为 .ZIP 存档。文件名称中的 XXXX 是序列号，每发布一个 DAT 版本，该号码也随之改变。要下载这些文件，请使用 Web 浏览器或 FTP 客户端登录：

  ftp://ftp.nai.com/antivirus/datfiles/4.x

- **可安装的 .EXE 文件**。McAfee 将这些文件存储在它的网站上，名为 XXXXUPDT.EXE，是自安装文件。这里的 XXXX 也是序列号，随每次新病毒定义文件的发布而更改。要下载这些文件，请使用 Web 浏览器登录：

  http://www.mcafeeb2b.com/naicommon/download/dats/find.asp

它们都包含完全相同的病毒定义文件。不同之处在于如何使用它们来更新您的 VirusScan Enterprise 软件。

要使用 DAT-XXXX.ZIP 存档，您必须下载并解压缩该文件、将文件复制到 DAT 目录中，然后重新启动按访问扫描程序。详细说明，请参阅第 173 页的 “从 DAT 文件存档更新”。

要安装安装程序附带的 DAT 文件，只需将文件下载到硬盘上的一个临时目录，然后运行或双击 XXXUPDT.EXE 文件。安装程序会停止按访问扫描程序、将文件复制到正确的目录中，然后重新启动按访问扫描程序。

注释
只有具有管理员权限，才能向 DAT 目录中写入。

更新之后，在按访问扫描程序、按需扫描程序和电子邮件扫描程序下次启动时，就会采用新的 DAT 文件。

从 DAT 文件存档更新

要直接从 .ZIP 存档安装 DAT 文件更新，同时不使用自动更新，请按照以下步骤执行。

1. 在硬盘中创建一个临时目录，然后将下载的 DAT 文件 .ZIP 存档复制到该目录下。
2. 备份或重命名现有的 DAT 文件。
   - CLEAN.DAT
   - NAMES.DAT
   - SCAN.DAT

   如果接受了默认的安装路径，这些文件将位于：

   驱动器 :\Program Files\Common Files\Network Associates\Engine
3. 使用 WINZIP、PKUNZIP 或类似的实用程序打开 .ZIP 存档并解压缩更新后的 DAT 文件。
4. 登录到您要更新的服务器。您必须对目标计算机拥有管理员权限。

5 将 DAT 文件复制到 DAT 目录中。

6 禁用按访问扫描程序，然后重新启动它。

7 停止 Microsoft Outlook，然后重新启动它。

8 停止按需扫描任务，然后重新启动它们。

计划任务

8

您可以计划在指定的日期和时间或按特定的时间间隔运行的任务。

这部分包含下列主题：

计划任务

您可以计划的任务共有三种：

- 按需扫描任务 - 要计划按需扫描任务，打开该任务的“**按需扫描属性**”，然后单击“**计划**”。“**计划设置**”对话框将打开。

  有关按需扫描任务的更多信息，请参阅第 63 页的“按需扫描”。

- 自动更新任务 - 要计划一个自动更新任务，请打开自动更新任务的“**自动更新属性**”，然后单击“**计划**”。“**计划设置**”对话框将打开。

  关于自动更新任务的更多信息，请参阅第 154 页的“自动更新”。

- 镜像任务 - 要计划一个镜像任务，请打开“**自动更新属性**”，然后单击“**计划**”。“**计划设置**”对话框将打开。

  关于镜像任务的更多信息，请参阅第 159 页的“镜像任务”。

这部分包含下列主题：

- 任务属性
- 计划属性

任务属性

使用“**任务**”选项卡上的此选项来启用计划，指定任务运行的时限，并输入该任务的身份验证。

1 选择“**任务**”选项卡。

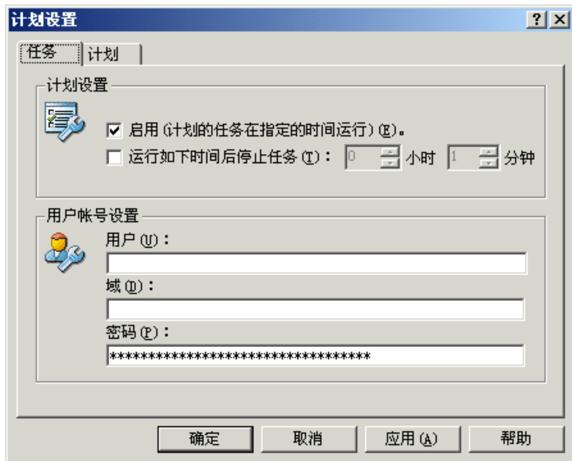


图 **8-1.** 计划设置 **-** 任务选项卡

2 在 **“计划设置”**区域中，指定是否希望任务在特定的时间运行。您可以选择以下选项：

- **启用 （计划的任务在指定时间运行）**。使任务在指定的时间运行。
- **运行如下时间后停止任务**。在限定的时间后停止任务。如果选择了该选项，还需输入 **“小时”**和 **“分钟”**。

注释
一旦任务在结束前中断，那么如果尚未更新 DAT 文件而且未选择在 DAT 文件更新之后重新扫描所有文件，则此次扫描将在下次启动时从中断处继续扫描。如果 DAT 文件已经更新并且选择了在 DAT 文件更新之后重新扫描所有文件，此次扫描将重新开始而不是从中断处继续。

3 在 **“用户帐号设置”**区域中，输入以下信息来指定该任务的身份验证证书：

注释
证书的使用是可选性的。如果您不在此处输入证书，则计划任务会在本地系统帐户下运行。

- **用户**。输入运行该任务的用户的 ID。
- **域**。输入指定的用户 ID 的域。
- **密码**。输入指定的用户 ID 和域的密码。

4 单击 **“应用”**保存更改。

注释
如果您使用了证书来计划任务，那么您指定的帐户需具有登录为批处理作业权限。没有此权限，即使具有正确的证书，生成的进程也无法访问网络资源。这是具有执照的 Windows NT 行为。

要赋予帐户此权限：

- **“开始”** | **“程序”** | **“管理工具”** | **“本地安全策略”**。
- **“安全设置”** | **“本地策略”** | **“用户权利指派”**。
- 双击 **“作为批处理作业登录”**。
- 将该用户添加至列表中。
- 单击 **“确定”**保存更改并关闭该对话框。

计划属性

使用 **“计划”**选项卡上的此选项来指定任务频率、任务在时区中运行的时间、是否在指定的间隔内随机运行任务、是否运行错过的任务，并指定错过任务的延迟时间。

这部分包含下列主题：

- 计划任务频率
- 高级计划选项
- 计划任务频率

计划任务频率

此处选择的计划频率会影响正在使用的计划日、周和月等选项。频率选项包括：

- **每天。**该选项为默认选项。在指定的那些天中，每天执行该任务。请参阅第 180 页的 “每天”。
- **每周**。在指定的星期和天中运行任务。请参阅第 181 页的 “每周”。
- **每月**。在指定的月份和天中运行任务。请参阅第 182 页的 “每月”。
- **一次**。在指定的日期运行一次任务。请参阅第 184 页的 “一次”。
- **系统启动时**。在系统启动时运行任务，并可指定是否每天运行一次该任务以及该任务延迟的分钟数。请参阅第 185 页的 “系统启动时”。
- **登录时**。在登录时运行任务，并可指定是否每天运行一次该任务以及该任务延迟的分钟数。请参阅第 186 页的 “登录时”。
- **空闲时**。在计算机空闲时运行任务，并可指定分钟数。请参阅第 187 页的“空闲时”。
- **立即运行**。该任务会立即运行。请参阅第 188 页的 “立即运行”。
- **拨号时运行**。在拨号时运行任务，并可指定是否每天运行一次该任务。请参阅第 189 页的 “拨号时运行”。

高级计划选项

1 在“**计划**”选项卡的“**计划**”区域中，单击“**高级**”打开“**高级计划选项**”对话框。



图 **8-2.** 高级计划选项

- **开始日期**。单击 ▼ 以便从日历中选择一个日期。该字段为可选项。
- **结束日期**。单击 ▼ 以便从日历中选择一个日期。该字段为可选项。
- **重复任务**。按照选定的频率重复运行任务。
- **每**。输入频率或通过箭头选择一个数值，然后选择频率是以分钟还是小时为单位。
- **直到**。选择“**时间（本地）**”并输入时间，或选择“**持续时间**”并输入“**小时**”和“**分钟**”。

2 单击“**确定**”返回到“**计划**”选项卡。

计划任务频率

您可以计划任务的运行日期和 / 或时间，以满足自己的需求。

这部分包含下列任务频率：

- 每天
- 每周
- 每月
- 一次
- 系统启动时
- 登录时
- 空闲时

- 立即运行
- 拨号时运行

每天

1 在 “**计划**” 选项卡的 “**计划任务**” 区域中：

- **计划任务**。单击▼选择 “**每天**”。

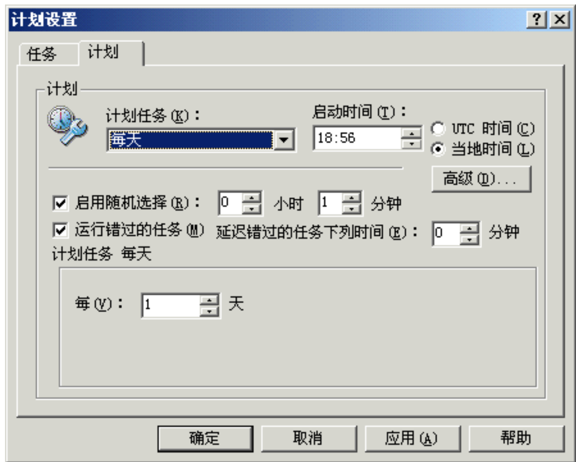


图 **8-3.** 计划选项卡 **-** 每天

- **启动时间**。输入计划任务的启动时间，或使用箭头选择时间。
- **UTC 时间**。通用协调时间 (UTC)。选择该选项将会在所有时区内同时运行任务。
- **当地时间**。该选项为默认选项。在每一个本地时区内独立运行该任务。
- **启用随机选择**。该任务将在指定的时间间隔内某个随机时刻运行。如果选择该选项，还需输入 “**小时**” 和 “**分钟**”，以便设置最大延迟时间。

  您可以输入时间间隔，介于 1 分钟和 24 小时之间。例如，将该任务的运行时间设置为 1:00，并将随机选择时段设置为三个小时，则会使该任务在 1:00 和 4:00 之间的任意时刻运行。
- **运行错过的任务**。可确保在计算机再次启动时运行错过的任务。如果计算机在任务的计划运行时间处于离线状态，这个任务将被错过。该功能可确保即使在远程用户和网络处于离线状态，而此时正值计划任务运行的时间，它们仍能受到完全保护。
- **延迟错过的任务下列时间**。在框中输入错过的任务的延迟分钟数，或使用箭头选择分钟数。

- **高级**。单击该按钮设置高级计划属性。更多信息，请参阅第 179 页的“高级计划选项”。

2 在 “**计划任务每天**” 中，输入计划任务间隔的天数，或者使用箭头选择一个数值。

注释
按天任务可每隔若干天运行一次，或从周一到周日每天都运行一次。如果您只想在每周指定的天中运行该任务，而不是从周一到周日每天都运行，那么我们建议您使用每周任务频率。

3 单击 “**确定**” 保存设置并关闭 “**计划设置**” 对话框。

每周

1 在 “**计划**” 选项卡的 “**计划任务**” 区域中：

- **计划任务**。单击▼选择 “**每周**”。

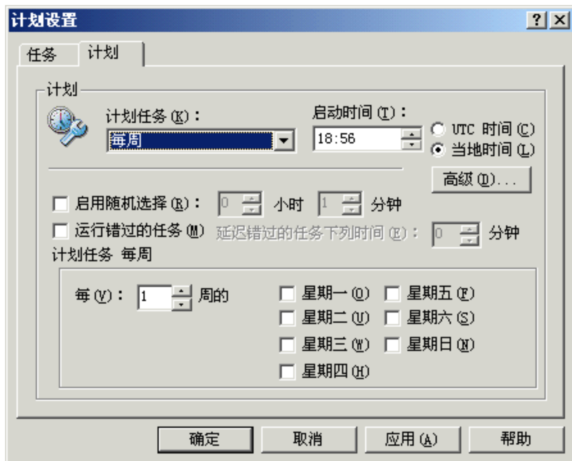


图 8-4. 计划选项卡 - 每周

- **启动时间**。输入计划任务的启动时间，或使用箭头选择时间。
- **UTC 时间**。通用协调时间 (UTC)。选择该选项将会在所有时区内同时运行任务。
- **当地时间**。该选项为默认选项。在每一个本地时区内独立运行该任务。
- **启用随机选择**。该任务将在指定的时间间隔内某个随机时刻运行。如果选择该选项，还需输入 “**小时**” 和 “**分钟**”，以便设置最大延迟时间。

您可以输入时间间隔，介于 1 分钟和 24 小时之间。例如，将该任务的运行时间设置为 1:00，并将随机选择时段设置为三个小时，则会使该任务在 1:00 和 4:00 之间的任意时刻运行。

- **运行错过的任务**。可确保在计算机再次启动时运行错过的任务。如果计算机在任务的计划运行时间处于离线状态，这个任务将被错过。该功能可确保即使在远程用户和网络处于离线状态，而此时正值计划任务运行的时间，它们仍能受到完全保护。
- **延迟错过的任务下列时间**。在框中输入错过的任务的延迟分钟数，或使用箭头选择分钟数。
- **高级**。单击该按钮设置高级计划属性。更多信息，请参阅第 179 页的 “高级计划选项”。

2 在 “**计划任务每周**” 区域中：

- **每**。输入计划任务间隔的星期数。
- **周的**。选择在星期几运行任务。

3 单击 “**确定**” 保存设置并关闭 “**计划设置**” 对话框。

每月

1 在 “**计划**” 选项卡的 “**计划任务**” 区域中：

- **计划任务**。单击选择 “**每月**”。

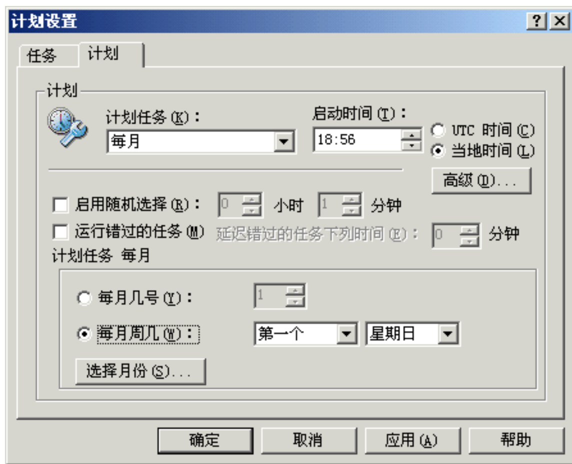


图 **8-5.** 计划选项卡 - 每月

- **启动时间**。输入计划任务的启动时间，或使用箭头选择时间。

- **UTC 时间**。通用协调时间 (UTC)。选择该选项将会在所有时区内同时运行任务。
- **当地时间**。该选项为默认选项。在每一个本地时区内独立运行该任务。
- **启用随机选择**。该任务将在指定的时间间隔内某个随机时刻运行。如果选择该选项，还需输入 “**小时**” 和 “**分钟**”，以便设置最大延迟时间。

  您可以输入时间间隔，介于 1 分钟和 24 小时之间。例如，将该任务的运行时间设置为 1:00，并将随机选择时段设置为三个小时，则会使该任务在 1:00 和 4:00 之间的任意时刻运行。
- **运行错过的任务**。可确保在计算机再次启动时运行错过的任务。如果计算机在任务的计划运行时间处于离线状态，这个任务将被错过。该功能可确保即使在远程用户和网络处于离线状态，而此时正值计划任务运行的时间，它们仍能受到完全保护。
- **延迟错过的任务下列时间**。在框中输入错过的任务的延迟分钟数，或使用箭头选择分钟数。
- **高级**。单击该按钮设置高级计划属性。更多信息，请参阅第 179 页的“高级计划选项”。

2 在 “**计划任务每月**” 区域中，选择下列选项之一：
   - **每月几号**。选择该选项指定每月运行任务的日期。
   - **每月周几**。选择该选项在每月的具体日期运行任务（例如第一个星期日、第二个星期三等）。
     - 选择选项 “**第一个**”、“**第二个**”、“**第三个**”、“**第四个**” 或 “**最后一个**”。
     - 选择各月中运行任务的周和天。
   - 单击 “**选择月份**” 选择具体月份：
     - 选择要运行任务的月份。

       注释
       默认选择所有月份。
     - 单击 “**确定**” 返回到 “**计划**” 选项卡。

3 单击 “**确定**” 保存设置并关闭 “**计划设置**” 对话框。

一次

1 在“**计划**”选项卡的“**计划任务**”区域中：

- **计划任务**。单击▼选择“**一次**”。

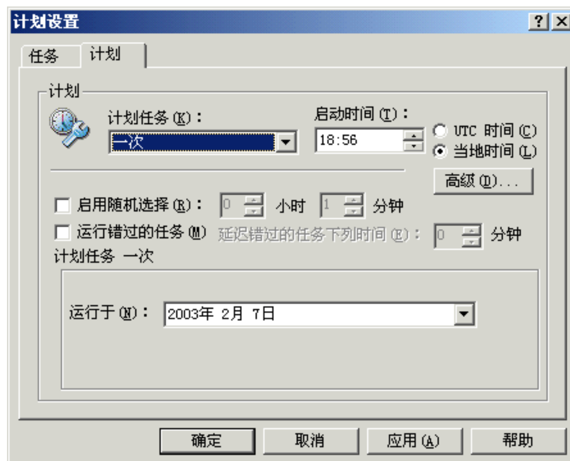


图 **8-6.** 计划选项卡 **-** 一次

- **启动时间**。输入计划任务的启动时间，或使用箭头选择时间。
- **UTC 时间**。通用协调时间 (UTC)。选择该选项将会在所有时区内同时运行任务。
- **当地时间**。该选项为默认选项。在每一个本地时区内独立运行该任务。
- **启用随机选择**。该任务将在指定的时间间隔内某个随机时刻运行。如果选择该选项，还需输入“**小时**”和“**分钟**”，以便设置最大延迟时间。

  您可以输入时间间隔，介于 1 分钟和 24 小时之间。例如，将该任务的运行时间设置为 1:00，并将随机选择时段设置为三个小时，则会使该任务在 1:00 和 4:00 之间的任意时刻运行。
- **运行错过的任务**。可确保在计算机再次启动时运行错过的任务。如果计算机在任务的计划运行时间处于离线状态，这个任务将被错过。该功能可确保即使在远程用户和网络处于离线状态，而此时正值计划任务运行的时间，它们仍能受到完全保护。
- **延迟错过的任务下列时间**。在框中输入错过的任务的延迟分钟数，或使用箭头选择分钟数。
- **高级**。单击该按钮设置高级计划属性。更多信息，请参阅第 179 页的“高级计划选项”。

2 在“**计划任务一次**”区域中，单击▼以选择运行任务的日期。

3 单击 “**确定**”保存设置并关闭 “**计划设置**”对话框。

系统启动时

1 在 “**计划**”选项卡的 “**计划任务**”区域中：

- **计划任务**。单击选择 “**系统启动时**”。

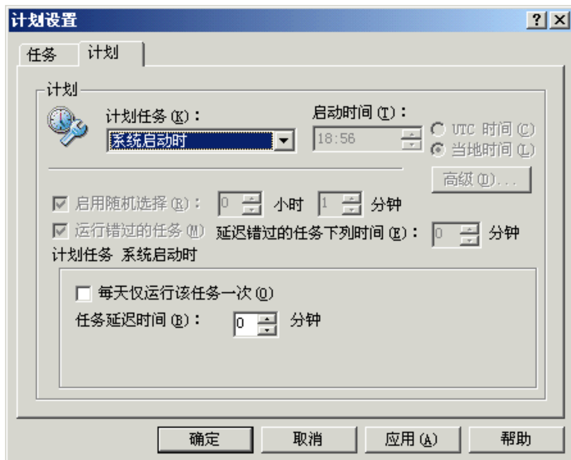


图 **8-7.** 计划选项卡 **-** 系统启动时

2 在 “**计划任务系统启动时**”区域中：

- **每天仅运行该任务一次。**选择此选项每天运行该任务一次。如果您不选择此选项，任务在每次启动时运行。
- **任务延迟时间。**选择任务延迟的分钟数。这给登录脚本的运行或用户登录空出了时间。

3 单击 “**确定**”保存设置并关闭 “**计划设置**”对话框。

登录时

1 在“**计划**”选项卡的“**计划任务**”区域中：

- **计划任务**。单击选择“**登录时**”。

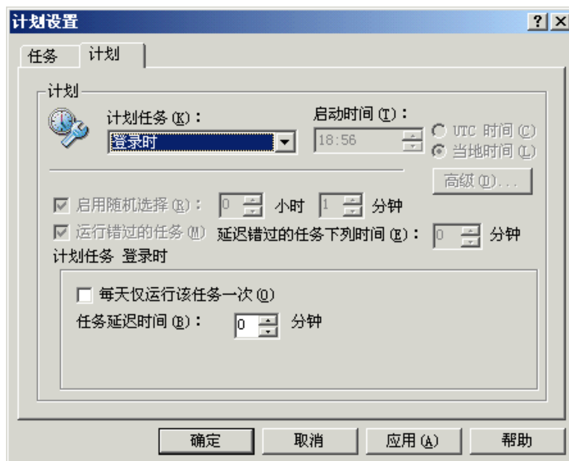


图 **8-8.** 计划选项卡 **-** 登录时

2 在“**计划任务登录时**”区域中：

- **每天仅运行该任务一次。**选择此选项每天运行该任务一次。如果您不选择此选项，任务在每次登录时运行。
- **任务延迟时间。**输入任务延迟的分钟数。这给登录脚本的运行或用户登录空出了时间。

3 单击“**确定**”保存设置并关闭“**计划设置**”对话框。

空闲时

1 在 “**计划**” 选项卡的 “**计划任务**” 区域中：

- **计划任务**。单击选择 “**空闲时**”。

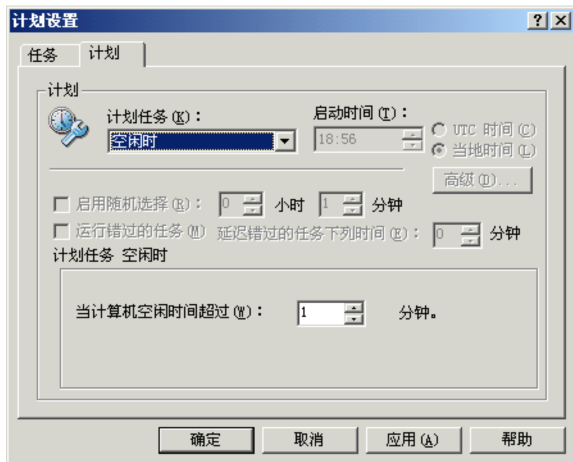


图 **8-9.** 计划选项卡 **-** 空闲时

2 在 “**计划任务空闲时**” 区域中，输入在启动任务之前计算机要保持空闲的分钟数。

3 单击 “**确定**” 保存设置并关闭 “**计划设置**” 对话框。

立即运行

1 在“**计划**”选项卡的“**计划任务**”区域中：

- **计划任务**。单击▼选择“**立即运行**”。

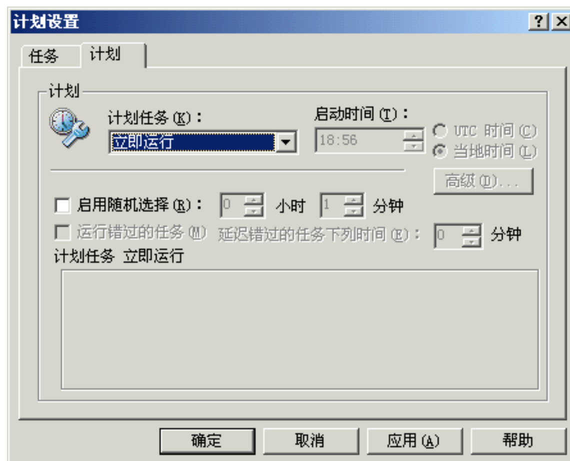


图 **8-10.** 计划选项卡 - 立即运行

- **启用随机选择**。该任务将在指定的时间间隔内某个随机时刻运行。如果选择该选项，还需输入“**小时**”和“**分钟**”，以便设置最大延迟时间。

  您可以输入时间间隔，介于 1 分钟和 24 小时之间。例如，将该任务的运行时间设置为 1:00，并将随机选择时段设置为三个小时，则会使该任务在 1:00 和 4:00 之间的任意时刻运行。

2 单击“**确定**”保存设置并关闭“**计划设置**”对话框。

拨号时运行

1 在 “**计划**” 选项卡的 “**计划任务**” 区域中：

- **计划任务。**单击▼选择 “**拨号时运行**”。

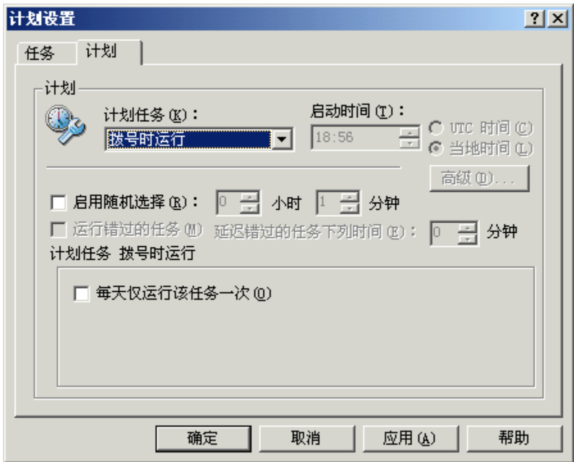


图 8-11. 计划选项卡 - 拨号时运行

- **启用随机选择**。该任务将在指定的时间间隔内某个随机时刻运行。如果选择该选项，还需输入 “**小时**” 和 “**分钟**”，以便设置最大延迟时间。

  您可以输入时间间隔，介于 1 分钟和 24 小时之间。例如，将该任务的运行时间设置为 1:00，并将随机选择时段设置为三个小时，则会使该任务在 1:00 和 4:00 之间的任意时刻运行。

2 在 “**计划任务拨号时运行**” 区域中，选择是否每天运行一次任务。

注释
与按需扫描任务相比，对于自动更新任务而言，将任务安排在 “**拨号时运行**” 更加有用。

3 单击 “**确定**” 保存设置并关闭 “**计划设置**” 对话框。

命令行扫描程序 A

VirusScan Enterprise 软件的典型安装包括 McAfee VirusScan Enterprise 命令行程序。该程序可以从 Windows 命令行提示符运行。

这部分包含下列主题：

- VirusScan Enterprise 命令行选项
- 按需扫描命令行选项
- 自定义安装属性

VirusScan Enterprise 命令行选项

要运行 VirusScan Enterprise 命令行程序，请打开 SCAN.EXE 所在的目录并键入 SCAN。如果已将 VirusScan Enterprise 软件安装到默认位置，则该文件应位于：

C:\Program Files\Common Files\Network Associates\Engine

下表列出了可以添加到 SCAN 命令中的选项。下面列出的所有选项可以用于配置按需和按访问扫描，除非另有说明。

表 A-1. VirusScan 命令行选项

命令行选项	描述
/? 或 /HELP	显示一个 VirusScan 命令行选项列表，各选项都有一个简短说明。 您可能会发现，向 VirusScan 程序创建的报告文件添加一组扫描选项会很有用。为此，在命令提示符中键入 scan /? /REPORT < 文件名 >。扫描报告的结果中附有此次扫描任务的所有可用选项。
/ADL	除了扫描在命令行中指定的其他任何驱动器之外，还扫描所有本地驱动器，包括压缩驱动器和 PC 卡，但不包括磁盘。 要同时扫描本地驱动器和网络驱动器，请在同一个命令行中同时使用 /ADL 和 /ADN 命令。
/ADN	除了扫描在命令行中指定的其他任何驱动器之外，还扫描所有网络驱动器（包括光驱）是否有病毒。 **注意：**要同时扫描本地驱动器和网络驱动器，请在同一个命令行中同时使用 /ADL 和 /ADN 命令。

表 **A-1. VirusScan** 命令行选项 （*续*）

命令行选项	描述
/ALERTPATH <dir>	将目录 <dir> 指定为由集中警报监控的远程 NetWare 卷或 Windows NT 目录的网络路径。 VirusScan 将在检测到感染病毒的文件后，向服务器发送一个 .ALR 文本文件。 从这个目录中， VirusScan Enterprise 将使用它的集中警报功能按照现有的配置来广播或编译警报和报告。 要求： ◆ 您必须对指定的目录具有写入权限。 ◆ 该目录必须含有 VirusScan Enterprise 自带的 CENTALRT.TXT 文件。
/ALL	通过扫描可能感染病毒的所有文件 （而不考虑扩展名）来覆盖默认的扫描设置。 **注意:** 使用 /ALL 选项将明显增加扫描所需的时间。请仅在发现或怀疑有病毒时使用该选项。 要获得当前的文件类型扩展名列表，请在命令提示符处运行 /EXTLIST。
/ANALYZE	设置本软件，以便对程序和宏使用完整的启发式扫描。 **注意：**/MANALYZE 仅针对宏病毒； /PANALYZE 仅针对程序病毒。
/APPEND	与 /REPORT < 文件名 > 一起使用，可将报告信息文本附加到指定的报告文件中，而不是覆盖它。
/BOOT	仅扫描引导扇区和主引导记录。
/CLEAN	清除所有感染病毒的文件和系统区域中的病毒。
/CLEANDOCALL	作为防范宏病毒的措施，当只查到一处病毒感染时，/CLEANDOCALL 将清除 Microsoft Word 和 Office 文档中的所有宏。 **注意:** 该选项可删除所有的宏，包括未被病毒感染的宏。
/CONTACTFILE < 文件名 >	发现病毒时显示 < 文件名 > 的内容。可为用户提供联系信息和遇到病毒后如何处理的说明。（McAfee 建议将 /LOCK 与该选项配合使用。） 该选项在网络环境中尤其有用，原因在于您可以在一个中央文件中方便地维护信息文本，而不必在每个工作站中进行维护。 **注意:** 在联系人信息中，除反斜线 (\) 以外的任何字符都有效。应将以斜线 (/) 或连字符 (-) 开头的信息放在引号内。

表 **A-1. VirusScan** 命令行选项 （*续*）

命令行选项	描述
/DAM	修复开关：如果发现感染了病毒的宏，将删除所有宏。如果没有找到任何感染了病毒的宏，就不会执行删除操作。 如果怀疑文件感染了病毒，可以选择从数据文件中剥离所有宏，以便将感染病毒的可能性降至最低。为了在感染病毒之前删除文件中的所有宏，请将该选项与 /FAM 配合使用： scan < 文件名 >/fam /dam 当这两个选项配合使用时，发现的所有宏都将被删除，而无论是否感染了病毒。
/DEL	永久删除感染病毒的文件。
/EXCLUDE < 文件名 >	不扫描 < 文件名 > 中列出的文件。 使用该选项可以将特定文件从扫描操作中排除。将要排除的每个文件的完整路径列在单独的一行中。可以使用通配符 * 和 ?。
/EXTLIST	使用该选项可以从当前DAT文件中获取当前的文件类型扩展名列表。
/FAM	查找所有宏：不只是怀疑感染了病毒的宏。将找到的所有宏都视为可能的病毒。除非与 /DAM 选项配合使用，否则不会删除找到的宏。 如果怀疑文件感染了病毒，可以选择从数据文件中剥离所有宏，以便将感染病毒的可能性降至最低。为了在感染病毒之前删除文件中的所有宏，请将该选项与 /FAM 配合使用： scan < 文件名 >/fam /dam 当这两个选项配合使用时，发现的所有宏都将被删除，而无论是否感染了病毒。
/FREQUENCY <n>	在上一次扫描操作 <n> 小时后不进行扫描。 在感染病毒风险很小的环境中，使用该选项可防止不必要的扫描。 值得一提的是，扫描频率越高，对病毒的防范越有效。
/HELP 或 /?	显示一个扫描选项列表，各选项都有一个简短说明。 您可能会发现，向 VirusScan 程序创建的报告文件添加一组扫描选项会很有用。为此，在命令提示符中键入 scan /? /REPORT < 文件名 >。扫描报告的结果中附有此次扫描任务的所有可用选项。

表 **A-1. VirusScan** 命令行选项 *（续）*

命令行选项	描述
/LOAD < 文件名 >	从指定的文件加载扫描选项。 使用该选项可通过从一个 ASCII 格式的文件中加载自定义设置来执行已配置好的扫描操作。
/MANALYZE	针对宏病毒启用启发式扫描。 **注意：**/PANALYZE 仅针对程序病毒； /ANALYZE 则同时针对程序和宏病毒。
/MANY	在单个驱动器上连续扫描多个磁盘。扫描程序将提示您指定每个磁盘。 使用该选项快速检查多个软盘。 如果从启动盘运行 VirusScan 软件且只有一个软驱，则无法使用 /MANY 选项。
/MOVE <dir>	将在扫描过程中发现的所有感染病毒文件移到指定的目录，同时保留驱动器盘符和目录结构。 **注意：**当主引导记录或引导扇区感染了病毒时，该选项不起作用，因为它们不是真正的文件。
/NOBEEP	禁止扫描程序发现病毒时发出声响。
/NOBREAK	扫描期间禁用 CTRL-C 和 CTRL-BREAK。 当使用 /NOBREAK 选项时，用户将无法停止正在运行的扫描操作。
/NOCOMP	跳过而不检查使用 LZEXE 或 PkLite 文件压缩程序压缩的可执行文件。 当不需要完全扫描时，这样做可以减少扫描时间。否则，在默认情况下， VirusScan 将在内存中解压缩每个文件并检查病毒签名，从而检查这些可执行文件或自解压文件的内部。
/NODDA	不进行直接磁盘存取。该选项可防止扫描程序访问引导记录。 增加这项功能的目的是使扫描程序能够在 Windows NT 下运行。 您可能需要对某些设备驱动的驱动器使用该选项。 当访问空光驱或空 Zip 驱动器时，将 /NODDA 与 /ADN 或 /ADL 开关配合使用可能会产生错误。如果发生这种错误，请键入 F （表示 “失败”）对错误信息作出响应以继续扫描。
/NOXMS	不使用扩展内存 (XMS)。

表 **A-1. VirusScan** 命令行选项 （*续*）

命令行选项	描述
/PANALYZE	针对程序病毒启用启发式扫描。 **注意：**/MANALYZE 仅针对宏病毒； /ANALYZE 则同时针对程序和宏病毒。
/PAUSE	启用屏幕暂停。 当扫描程序在屏幕上显示信息时，将出现“按任意键继续”的提示。否则，默认情况下，扫描程序将不停顿地连续显示信息并滚动屏幕，这使它可以在具有多个驱动器或严重感染的计算机上运行，而不需要用户的输入。 McAfee 建议当使用报告选项（/REPORT、/RPTALL、/RPTCOR 和 /RPTERR）时都略去 /PAUSE。
/REPORT < 文件名 >	针对感染病毒的文件和系统错误创建报告，并以 ASCII 文本文件格式将数据保存到 < *文件名* > 中。 如果 < *文件名* > 已存在， /REPORT 将覆盖它。要避免覆盖，请将 /APPEND 与 /REPORT 配合使用：这样，本软件会将报告信息添加到文件末尾，而不会覆盖。 也可以使用 /RPTALL、/RPTCOR 和 /RPTERR 向报告中添加已扫描的文件、已损坏的文件、已修改的文件和系统错误。 您可能会发现，向 VirusScan 程序创建的报告文件添加一组扫描选项会很有用。为此，在命令提示符中键入 /? /report < *文件名* >。扫描报告的结果中附有此次扫描任务的所有可用选项。 可以包括目标驱动器和目录 （例如 D:\VSREPRT\ALL.TXT），但如果目标是网络驱动器，则必须具有在该驱动器上创建和删除文件的权限。 McAfee 建议在使用任何报告选项时都忽略 /PAUSE。
/RPTALL	将已扫描过的所有文件名附加到 /REPORT 文件中。 可以在同一个命令行中使用 /RPTERR 和 /RPTCOR 选项。 McAfee 建议在使用任何报告选项时都忽略 /PAUSE。

表 A-1. VirusScan 命令行选项 *（续）*

命令行选项	描述
/RPTCOR	将已损坏的文件附加到 /REPORT 文件中。 当与 /REPORT 配合使用时，该选项可以向报告文件中添加已损坏的文件的名称。 VirusScan 扫描程序发现的已损坏的文件可能是因病毒感染引起的。 可以在同一个命令行中使用 /RPTERR 和 /RPTCOR 选项。 某些文件中可能有错误的内容，这些文件需要被覆盖或者用另一个可执行文件才能正确运行（即该文件不能自己执行）。 McAfee 建议在使用任何报告选项时都忽略 /PAUSE。
/RPTERR	将错误附加到 /REPORT 文件中。 在与 /REPORT 配合使用时，该选项可向报告文件中添加已损坏的文件的名称。 /LOCK 适用于非常容易受攻击的网络环境，例如开放的计算机实验室。 可以在同一个命令行中使用 /RPTERR 和 /RPTCOR。 系统错误可以包括读取或写入磁盘或硬盘错误、文件系统问题或网络问题、创建报告时的问题以及与系统有关的其他问题。 McAfee 建议在使用任何报告选项时都忽略 /PAUSE。
/SUB	扫描目录内的子目录。 默认情况下，如果指定要扫描的是目录而非驱动器，VirusScan 扫描程序将只检查该目录所包含的文件，而不检查其子目录。 使用 /SUB 可以扫描任何指定目录中的所有子目录。如果指定扫描整个驱动器，则没有必要使用 /SUB 选项。
/UNZIP	扫描压缩文件内部。
/VIRLIST	显示 VirusScan 扫描程序检测到的每个病毒的名称。 此文件很大，可能超过 250 页，因此 MS-DOS“编辑”程序无法打开它； McAfee 建议使用 Windows 的 “记事本”或其他文本编辑器来打开病毒列表。

按需扫描命令行选项

VirusScan Enterprise 按需扫描程序可以从 Windows 命令行提示符或 “**开始**”菜单的 “**运行**”对话框中运行。要运行该程序，请打开 SCAN32.EXE 文件所在的目录，并键入 SCAN32。如果已将 VirusScan Enterprise 软件安装到默认位置，则该文件应位于：

C:\Program Files\Network Associates\VirusScan

下表列出了可以添加到 SCAN32 命令中的选项。

表 A-2. 按需扫描命令行参数

命令行选项	描述
SPLASH	打开按需扫描程序时，显示 VirusScan 启动屏幕。
NOSPLASH	打开按需扫描程序时，隐藏 VirusScan 启动屏幕。
AUTOSCAN	启动按需扫描程序并立即执行默认的扫描任务，而无需用户进一步干涉。
NOAUTOSCAN	既不启动按需扫描程序，也不自动执行任何扫描任务。 默认状态取决于 UI 设置： ◆ 如果 UI=none 或 UICONFIG，则 Autoscan=NO ◆ 如果 UI=EXONLY，则 Autoscan=YES ◆ 如果 UI=NONE，则 Autoscan=YES
AUTOEXIT	在非交互式扫描结束后，退出按需扫描程序。
NOAUTOEXIT	在非交互式扫描结束后，不退出按需扫描程序。
ALWAYSEXIT	强制退出按需扫描操作，即使扫描完成而且发生错误或扫描失败。
NOALWAYSEXIT	不强制退出。
UICONFIG	启动扫描程序，并使它的配置对话框可用。
UIEXONLY	启动扫描程序，并执行默认的扫描，但使配置对话框不可用。
UINONE	启动扫描程序，但使配置对话框不可用。这个参数要求输入其他参数来确定扫描目标。
SUB	扫描目标文件夹的子文件夹。
NOSUB	不扫描目标文件夹的子文件夹。

表 **A-2.** 按需扫描命令行参数 （*续*）

命令行选项	描述
ALL	扫描目标文件夹中的所有文件
NOALL	仅扫描目标文件夹中具有指定文件类型列表中所列文件扩展名的那些文件。
COMP	扫描存档文件，例如 .ZIP、.CAB、.LZH 和 .UUE 文件。
NOCOMP	不扫描存档文件。
CONTINUE	检测到病毒后继续扫描。
PROMPT	提示用户检测到病毒时采取何种操作。
NOPROMPT	不提示用户检测到病毒时采取何种操作。
CLEAN	检测到病毒时清除目标文件的病毒。
DELETE	检测到病毒时删除感染病毒的文件。
MOVE	检测到病毒时，将感染病毒的文件移动（隔离）到预先指定的隔离文件夹。
BEEP	如果扫描结束后发现感染病毒的项目，则发出蜂鸣声。
NOBEEP	即便扫描结束后发现感染病毒的项目，也不发出蜂鸣声。
RPTSIZE	设置警报日志的大小，单位为千字节。
BOOT	在运行当前扫描任务之前，扫描引导扇区。
NOBOOT	不扫描引导扇区。
EXT	您在该参数后面作为参数添加的文件扩展名将取代扫描时所用的所选文件类型列表中的扩展名。
DEFEXT	您在该参数后面作为参数添加的文件扩展名将添加到扫描时所用的所选文件类型列表中。
TASK	启动在 VirusScan Enterprise 控制台中指定的按需扫描程序任务。要求其他参数，以便在如下注册表位置中指定特定的任务 ID： HKEY_LOCAL_MACHINE;SOFTWARE; NETWORK ASSOCIATES;TVD; VirusScan EnterpriseNT; CurrentVersion;Tasks。
SERVER	该参数指定在哪台计算机上启动或停止扫描任务。

表 **A-2.** 按需扫描命令行参数 （*续*）

命令行选项	描述
CANCEL	如果任务失败但控制台仍表明它在运行，可使用该参数调整注册表，以便显示该任务不再运行。
LOG	在事先指定的日志文件中记录感染报告。
NOLOG	不记录感染报告。
LOGALL	将对病毒感染作出的所有响应都作为事件记录下来。包含提示、清除、删除和移动。
LOGDETECT	将病毒检测作为事件记录。
NOLOGDETECT	不将病毒检测作为事件记录。
LOGCLEAN	无论是否成功清除病毒，都将清除活动作为事件记录。
NOLOGCLEAN	无论是否成功清除病毒，都不将清除活动作为事件记录。
LOGDELETE	将删除感染病毒文件这一操作作为事件记录。
NOLOGDELETE	不将删除感染病毒文件这一操作作为事件记录。
LOGMOVE	将感染病毒文件移到隔离文件夹这一操作作为事件记录。
NOLOGMOVE	不将感染病毒文件移到隔离文件夹这一操作作为事件记录。。
LOGSETTINGS	记录扫描任务的配置设置。
NOLOGSETTINGS	不记录扫描任务的配置设置。
LOGSUMMARY	记录扫描任务结果的摘要。
NOLOGSUMMARY	不记录扫描任务结果的摘要。
LOGDATETIME	记录扫描活动的日期、开始时间和结束时间。
NOLOGDATETIME	不记录扫描活动的日期或时间。
LOGUSER	记录执行扫描任务的用户的识别信息。
NOLOGUSER	不记录用户信息。
PRIORITY	设置扫描任务相对于其他 CPU 进程的优先级。要求其他数值型参数。值为 1 时，为所有其他 CPU 进程指派优先级。值为 5 时，为扫描任务指派最高优先级。

自定义安装属性

从命令行安装时，您可以用特定属性自定义安装过程。

表 A-3. 安装自定义属性

命令行属性	功能
PRESERVESETTINGS	升级 NetShield 4.5 或 VirusScan 4.5.1 时保留设置。 False = False 值无法设置。 True = 保留设置。这是默认设置。 **注意：**如果不想保留设置，请将属性设置为 ""。字面上的含义是 PRESERVESETTINGS=""，一个空字符串。
INSTALLDIR	设置默认安装目录。
INSTALLALERTMANAGER	False = 不安装警报管理器 4.7。 True = 安装警报管理器 4.7，如果有。 如果在工作站上安装，默认值为 False ；如果在服务器上安装，默认值为 True。
ALERTMANAGERSOURCEDIR	设置默认警报管理器源路径。默认路径为 \AMG。 您可以在 SETUP.INI 中自行设置。
INSTALL_SITEINFO_FILE	导入自动更新资料库列表 (SITELIST.XML)。 False = False 值无法设置。 True = 导入 SITELIST.XML。文件已存在于指定路径中。 **注意:** 如果不想导入自动更新资料库列表，请将属性设置为 ""。字面上的含义是 INSTALL_SITEINFO_FILE=""，一个空字符串。
CMASOURCEDIR	为 SITELIST.XML 设置源路径。默认路径是 SETUP.EXE 正在运行的当前目录。
LOCKDOWNVIURUSSCANSHORTCUTS	False = False 值无法设置。 True = 在开始菜单下不显示任何快捷方式。 **注意：**如果希望允许安装快捷方式，请将属性设置为 ""。字面上的含义是 LOCKDOWNVIURUSSCANSHORTCUTS=""，一个空字符串。这是默认设置。

表 **A-3.** 安装自定义属性

命令行属性	功能
VIRUSSCANICONLOCKDOWN	以两种不同级别锁定产品。 NORMAL = 在系统任务栏的 VirusScan 图标菜单上显示所有菜单项。这是默认设置。 MINIMAL = 在系统任务栏的 VirusScan 图标菜单上仅显示 “**启用按访问扫描**” 和 “**关于 VirusScan Enterprise**” 菜单项。 NOICON = 在系统任务栏中不显示 VirusScan 图标菜单。
ENABLEONACCESSSCANNER	False = False 值无法设置。 True = 安装结束后启用按访问扫描程序。这是默认设置。 **注意：**如果不想启用按访问扫描程序，请将属性设置为 ""。字面上的含义是 ENABLEONACCESSSCANNER=""，一 个空字符串。
RUNAUTOUPDATE	False = False 值无法设置。 True =安装完成后运行更新。这是默认设置。 **注意：**如果完成安装后，不想运行更新，请将属性设置为 ""。字面上的含义是 RUN 自动更新 =""，一个空字符串。
RUNONDEMANDSCAN	False = 安装结束后不扫描所有本地驱动器。 True = 安装结束后扫描所有本地驱动器。这是默认设置。
RUNAUTOUPDATESILENTLY	False =不在安装结束后运行病毒定义文件静默更新。这是默认设置。 True = 安装完成后运行静默更新。
RUNONDEMANDSCANSILENTLY	False = 完成安装后，不运行静默按需扫描。这是默认设置。 True = 安装结束后运行静默按需扫描。

安全注册表 B

VirusScan Enterprise 程序与 Windows 安全注册表功能兼容。该程序将基于用户的安全许可权限写入注册表项。用户无权使用的任何程序功能都将呈现为灰色，表示不可选择或无响应。旧版产品有时会在 VirusScan Enterprise 程序试图为用户无权使用的某个功能写入注册表项时出错。

要了解 VirusScan Enterprise 程序及其警报管理器组件对哪些注册表键要求“写入”权限，请参阅要求写权限的注册表键。该表格还显示了权限不足的用户写入这些键值时的结果。

要求写权限的注册表键

本表显示的所有注册表键均为子键，主键为：

hkey_local_machine\software\network associates\tvd

表 B-1. VirusScan Enterprise 注册表键锁定的结果

功能	程序 或 Windows 服务	描述	需要写权限以获得全部功能的注册表键	当由于注册表锁定而没有 “写权限”时的结果
按访问扫描程序	Network Associates McShield 服务	只能使用本地系统帐户运行的一项 Windows 服务。这项服务会在使用某个文件时执行扫描。	Shared Components On-Access Scanner	由于这项服务只在使用“系统”帐户时运行，因此通常不受影响。然而，如果这项服务对该键值不具有写权限，则按访问扫描程序不起作用。
按访问扫描程序	ShCfg32.exe	一个可以运行按访问配置界面的程序。	Shared Components On-Access Scanner McShield Configuration	用户可以看到按访问扫描程序属性页，但不能更改配置。

表 **B-1. VirusScan Enterprise** 注册表键锁定的结果 *（续）*

功能	程序 或 **Windows** 服务	描述	需要写权限以获得全部功能的注册表键	当由于注册表锁定而没有 "写权限" 时的结果
按访问扫描程序	ShStat.exe	该程序汇集了按访问扫描程序活动的统计信息。该程序还将 VirusScan Enterprise 图标放在了系统任务栏中。通过右键单击该图标，用户可以查看扫描统计信息、禁用和启用该程序以及打开若干个程序组件。	Shared Components On-Access Scanner McShield Configuration	用户无法使用系统任务栏中的图标启用或禁用按访问扫描程序。
按需扫描程序	ScnCfg32	一个可以运行按需配置界面的程序。可以从 VirusScan Enterprise 控制台访问该界面。	VirusScan Enterprise CurrentVersion VirusScan Enterprise CurrentVersion Tasks VirusScan Enterprise CurrentVersion DefaultTask VirusScan Enterprise CurrentVersion Tasks	如果无法对这些键值中的任何一个进行写访问，用户还是可以看到按需扫描程序属性页，但不能更改配置。

表 **B-1. VirusScan Enterprise** 注册表键锁定的结果 *（续）*

功能	程序 或 **Windows** 服务	描述	需要写权限以获得全部功能的注册表键	当由于注册表锁定而没有 “写权限” 时的结果
按需扫描程序	ScnStat.exe	该程序汇集了按需扫描程序活动的统计信息。	VirusScan Enterprise CurrentVersion Tasks VirusScan Enterprise CurrentVersion VirusScan Enterprise CurrentVersion Tasks	无效
按需扫描程序	Scan32.exe	是可以对在 VirusScan Enterprise 控制台中指定的目标执行按需扫描活动的程序。	VirusScan Enterprise CurrentVersion VirusScan Enterprise CurrentVersion\\ Tasks **注意：**还要求对以下各项具有 “读” 权限： ◆ Shared Components ◆ VirusScan Engine ◆ 4.0.xx	如果 Scan32 对自身的任务不具有可写键值，则它将运行 （但不更新）统计信息或者生成扫描结果数据。 这不影响由下述任务管理器服务管理的事先计划的按需扫描任务。

表 **B-1. VirusScan Enterprise** 注册表键锁定的结果 *（续）*

功能	程序 或 **Windows** 服务	描述	需要写权限以获得全部功能的注册表键	当由于注册表锁定而没有 “写权限” 时的结果
任务 管理器	Network Associates 任务管理器服务	是可以使用 “系统” 帐户或 “管理员” 帐户运行的一项 Windows 服务。该程序允许计划扫描和更新活动。	VirusScan Enterprise NT CurrentVersion VirusScan Enterprise NT CurrentVersion Alerts VirusScan Enterprise NT CurrentVersion Tasks 所有子键 Shared Components On-Access Scanner McShield Shared Components On-Access scanner McShield Configuration	因为此服务只在使用系统或管理员帐户时运行，所以通常不受影响。然而，如果这项服务对这些键值中的任何一个不具有读 / 写权限，则该服务无法启动。

表 **B-1. VirusScan Enterprise** 注册表键锁定的结果 *（续）*

功能	程序 或 **Windows** 服务	描述	需要写权限以获得全部功能的注册表键	当由于注册表锁定而没有“写权限”时的结果
McUpdate	McUPdate.exe	用来更新病毒定义文件和软件升级的一个程序。	VirusScan Enterprise NT Current Version Shared Components On-Access Scanner McShield Configuration VirusScan Enterprise NT CurrentVersion Tasks VirusScan Enterprise NT CurrentVersion Tasks Update VirusScan Enterprise NT CurrentVersion Tasks Upgrade	DAT 信息不会更新 McShield 可能不会重新加载 DAT。 状态信息无法被发送到 VirusScan Enterprise 控制台。 用户可以看到更新属性页，但不能更改配置。 用户可以看到升级属性页，但不能更改配置。

表 **B-1. VirusScan Enterprise** 注册表键锁定的结果 （*续*）

功能	程序 或 **Windows** 服务	描述	需要写权限以获得全部功能的注册表键	当由于注册表锁定而没有 “写权限”时的结果
VirusScan Enterprise 控制台	McConsol.EXE	是可以运行 VirusScan Enterprise 程序管理界面的一个程序。	VirusScan Enterprise NT CurrentVersion	病毒定义更新功能不能可靠地运行。此外，用户还能看到当前屏幕的刷新率，但不能更改它。
			VirusScan Enterprise NT CurrentVersion Alerts CurrentVersion	通过选择 “**工具**”菜单中的 “**警报**”而可见的警报管理器设置将显示为灰色，而且即使被选择也不会作出响应。同时，由 VirusScan Enterprise 控制台控制的部分启动 / 停止任务也许无法生成。
			VirusScan Enterprise NT CurrentVersion Tasks	
			Shared Components On-Access Scanner McShield Configuration	下列选项将变灰，而且即使被选择也不会作出响应： ◆ 启用 / 禁用按访问扫描任务。 ◆ 复制、粘贴、删除、重命名、导入和导出任务 ◆ 停止扫描控制
			VirusScan Enterprise NT CurrentVersion Tasks Xxxx	无法配置、启用或禁用按访问扫描任务。 无法配置锁定的任何键。
警报管理器	NAI 警报 管理器	一个当扫描程序检测到病毒、或者事件计划程序遇到问题后能够立即发出通知的组件。	Shared Components Alert Manager	用户可以看到警报方法和消息的属性页，但不能更改配置。

故障排除 C

本节讲述有关 VirusScan Enterprise 产品的故障排除信息。

这部分包含下列主题：

- Minimum Escalation Tool
- 常见问题

Minimum Escalation Tool

McAfee Minimum Escalation Tool (MERTool，最小扩展工具) 作为一款实用程序，专门用于收集系统上有关 Network Associates 软件的报告和日志。它获取的信息有助于分析问题。

要获得有关 MERTool 的更多信息并访问该实用程序，请单击与 VirusScan Enterprise 产品一起安装的 MERTool 文件。

本文件位于安装目录。如果接受了默认的安装路径，本文件位于：

驱动器 :\Program Files\Common Files\Network Associates\VirusScan

当您单击 MERTool 文件时，它会访问 MERTool 网站的 URL。按照网站上的说明进行操作。

常见问题

本节以常见问题的形式讲述故障排除信息。问题分为以下种类：

- 安装问题
- 扫描问题
- 病毒问题
- 常规问题

安装问题

我刚刚使用 “静默安装”方法安装完本软件，但是在 Windows 系统任务栏中没有 VirusScan Enterprise 图标。

重新启动系统后，图标才会出现在系统任务栏中。但是，即使没有图标，VirusScan Enterprise 仍在运行，且您的计算机受到保护。

为什么网络中有部分用户可以在 VirusScan Enterprise 中配置自己的设置，而其他用户不可以？

不同的 Microsoft Windows 操作系统有不同的用户权限。 Windows NT 用户有权限写入系统注册表，而 Windows XP 或 Windows 2000 用户没有。请参阅 Microsoft Windows 文档，了解有关用户权限的详细信息。

在命令行安装过程中，如何防止没有管理权限的用户通过 VirusScan 控制台获得管理权限？

添加下面的属性可以在命令行安装过程中防止用户获得管理权限：

DONOTSTARTSHSTAT=True

这可以防止 SHSTAT.EXE 在完成安装后启动。

扫描问题

在按访问扫描中，“写入磁盘时”扫描与 “读取磁盘时”扫描有什么区别？

写入时扫描是文件写入操作。它扫描以下项目：

- 写入本地硬盘驱动器的进入文件。
- 在本地硬盘驱动器或映射的网络驱动器上创建的文件 （这包括新文件、修改的文件或者从一个驱动器复制或移动到另一个驱动器的文件）。

读取时扫描是文件读取操作。它扫描以下项目：

- 从本地硬盘驱动器读取的外出文件。

  注释
  在 “**按访问扫描属性**”对话框中选择 “**在网络驱动器上**”以包括远程网络文件。

- 在本地硬盘驱动器上执行的任何文件。
- 在本地硬盘驱动器上打开的任何文件。
- 在本地硬盘驱动器上重命名的任何文件，如果属性已更改。

当我使用 “按需电子邮件扫描”或 “按发送电子邮件扫描”检测到病毒时，这两个

操作选项有什么区别？

请参阅第 109 页的 “操作属性”了解每个操作选项的详细说明。

病毒问题

我怀疑感染上病毒，但是 VirusScan Enterprise 未检测到。

您可以下载最新的 DAT 文件，但该文件可能正在测试中，尚未正式发布。要使用每日的 DAT 文件，请参考：

www.mcafeeb2b.com/naicommon/avert/avert-research-center/virus-4d.asp

我无法安装 VirusScan Enterprise，我想可能感染了病毒。我怎么知道我的计算机是否感染病毒？

如果您不能安装 VirusScan Enterprise，仍可以用命令行运行扫描，使用从 Network Associates 网站下载的单个文件。要在尚未安装防病毒软件的计算机上运行命令行扫描：

1. 在 C 驱动器的根目录下创建一个名为 Scan 的文件夹。
2. 右键单击 Scan 文件夹并选择 “**属性**”。确保选定只读属性。
3. 转到 http://nai.com/naicommon/download/dats/superdat.asp
   单击 **sdatxxxx.exe for Windows-Intel** 开始下载。
4. 将此文件下载到新文件夹 (`C:\Scan`)
5. 从“**开始**”菜单，选择“**运行**”并在文本框中键入 `C:\Scan\sdatxxxx.exe /e`。单击 “**确定**”。
6. 打开DOS提示符（也称为“**命令提示符**”）。在`C:\>`提示符下，键入`cd c:\Scan`
   现在的提示符为：`C:\Scan>`
7. 在 `C:\Scan>` 提示符下，键入：

   scan.exe /clean /all /adl /unzip /report report.txt

   这会扫描所有本地驱动器并创建一个报告，文件名为 REPORT.TXT。
8. 扫描后，浏览到 `C:\Scan` 目录，查看 REPORT.TXT 文件。

> **注释**
>
> 我们建议您在扫描之前断开系统与网络的连接。
>
> 在 Windows 2000 和 Windows XP 系统上，重新启动进入 “纯 DOS 模式”执行扫描。在 Windows NT 系统上，从 VGA 模式下运行扫描，然后执行命令提示符扫描。
>
> 我们建议在找不到病毒后再返回命令行扫描程序。您可以将报告文本文件重命名为 REPORT2.TXT 记录第二次扫描，重命名为 REPORT3.TXT 记录第三次扫描，依此类推，避免每次覆盖报告文件。

警告
您可能会看到一条错误消息提示，有一个应用程序试图直接访问 Windows NT 系统上的硬盘。单击 “**忽略**”，或扫描终止。

常规问题

我系统任务栏中的 VirusScan Enterprise 图标好像被禁用了。

如果 VirusScan Enterprise 图标上有红圈和横线，就表示 “按访问扫描” 被禁用。这就是一些最常见的原因和解决方案。如果这些方法都无法解决您的问题，请与技术支持联系。

- 确保 “按访问扫描” 已启用。为此：
  - 右键单击系统任务栏中的 VirusScan Enterprise 图标。如果按访问扫描程序被禁用，文字 “**启用按访问扫描**” 会出现在菜单上。
  - 选择 “**启用按访问扫描**” 选项启用按访问扫描程序。
- 确保服务正在运行。为此：
  - 使用以下方法打开 “**控制面板**” 中的 “**服务**”：
    - 对于 Windows NT，选择 “**开始**” | “**设置**” | “**控制面板**” | “**服务**”，确认 **Network Associates MCShield** 的 “**状态**” 为 “**启动**”。
    - 对于 Windows 2000 或 XP，选择 “**开始**” | “**设置**” | “**控制面板**” | “**管理工具**” | “**服务**”，确认 **Network Associates MCShield** 的 “**状态**” 为 “**启动**”。
  - 若尚未启动，请突出显示服务列表上的 **Network Associates MCShield**，单击 “**开始**” 或 “**更新**”。
- 确保服务设置为自动启动。为此：
  - 使用以下方法打开 “**控制面板**” 中的 “**服务**”：
    - 对于 Windows NT，选择 “**开始**” | “**设置**” | “**控制面板**” | “**服务**”，确认 **Network Associates McShield** 的 “**状态**” 或 “**启动类型**” 为 “**自动**”。

      如果不是 “**自动**”，请突出显示服务列表上的 **Network Associates McShield**，单击 “**启动**” 并选择 “**自动**”。
    - 对于 Windows 2000 或 XP，选择 “**开始**” | “**设置**” | “**控制面板**” | “**管理工具**” | “**服务**”，确认 **Network Associates McShield** 的 “**状态**” 或 “**启动类型**” 为 “**自动**”。

      如果不是 “**自动**”，请右键单击服务列表上的 **Network Associates McShield**，然后单击 “**属性**”，在 “**常规**” 选项卡上选择 “**自动**” 作为 “**启动类型**”。

我得到错误消息说我不能下载 catalog.z。

发生这个错误的原因很多。以下给出一些有助于您找出问题的原因的建议。

- **如果使用 Network Associates 默认更新站点**，决定是否通过 web 浏览器来下载 `catalog.z` 文件。要这样做，请前往 URL http://download.nai.com/products/commonupdater/catalog.z 然后尝试下载此文件。
    - 如果**不能**下载此文件但是可以看到它（换句话说，您的浏览器不支持下载），这意味您的代理服务器出现问题，需要告知网络管理员。
    - 如果**能**下载此文件，这意味 VirusScan Enterprise 7.0 也应该能够下载这个文件。与您的技术支持联络，让他们帮助您排除安装 VirusScan Enterprise 时发生的故障。
- **如果使用镜像更新站点**，确保镜像站点指向正确的更新站点。如果没有把握，尝试更改您的设置以便使用默认的 Network Associates 站点。

我有些计算机继续使用 VirusScan 4.5x，而其他一些则使用 VirusScan Enterprise 7.0。是否所有的计算机都能够使用相同的 DAT 资料库？

是的，运行多版本的 VirusScan 的计算机网络可使用相同的 DAT 资料库。为此，请确保已经在 McAfee AutoUpdate Architect 控制台中，选择了“**我需要使我的站点与原有软件兼容**”。更多信息，请参阅 《McAfee AutoUpdate Architect 产品指南》。

HTTP DAT 文件的位置在哪里？

DAT 文件可从以下 web 站点下载：

```
http://download.nai.com/products/commonupdater/catalog.z
```

FTP 站点的位置在哪里？

DAT 文件可从以下 FTP 站点下载：

```
ftp://ftp.nai.com/commonupdater/catalog.z
```

如果我确实发现了病毒，而且已经选择 “提示用户操作”，我该选择什么操作 （清除、删除、移动）？

如果您没有把握该对染毒文件如何操作，我们一般建议选择 “**清除**”。 VirusScan Enterprise 默认操作是清除文件病毒，然后移动它。

我试图 “移动”或 “删除”文件，但没有成功。

这可能是由于文件被另一个程序锁定，或者您没有权限移动或删除这个文件。如果在工作区，您可以查找 VirusScan Enterprise 日志并查看该文件位置，然后使用 Windows 资源管理器手动移动或删除该文件。

索引

F

G

H

J

K

L

M

P

Q

R

S